



FFI-RAPPORT

17/00182

Hvordan kan vi kommunisere det vi ikke vet?

En kvalitativ studie om risikoforståelse og risikokommunikasjon i en terrorismekontekst

—
Janita Andreassen Bruvoll

**Hvordan kan vi kommunisere det vi
ikke vet?
En kvalitativ studie om risikoforståelse og
risikokommunikasjon i en terrorismekontekst**

Janita Andreassen Bruvoll

Emneord

Risikovurdering
Terrorisme
Kommunikasjon

FFI-rapport

FFI-RAPPORT 17/00182

Prosjektnummer

1391

ISBN

P: 978-82-464-2892-5

E: 978-82-464-2893-2

Godkjent av

Kjersti Brattekås, *forskningsleder*

Janet M. Blatny, *avdelingssjef*

Sammen drag

Trusselbildet i Norge er endret, og oppmerksomheten rundt tilsiktede uønskede handlinger, særlig terrorhandlinger, har økt. Hendelser som 11. september 2001, 22. juli 2011 og angrepet i In Amenas i 2013 har endret vår risikopersepsjon, og vist at terrorangrep både kan skje her hjemme og ramme norske interesser i utlandet. Diskusjonen rundt hvorvidt og hvordan risikoen for tilsiktede uønskede handlinger kan styres, har vært aktuell på politisk og strategisk nivå, i akademia og media.

Det er bred enighet om at stor grad av usikkerhet er det som skiller tilsiktede uønskede handlinger fra utilsiktede hendelser. Usikkerheten gjelder særlig risikoen for terrorhandlinger. Denne studien retter oppmerksomheten mot risikoforståelse og risikokommunikasjon og hvordan dette fungerer i en terrorismekontekst. **Hovedformålet med studien er å besvare spørsmålet om hvordan usikkerheten i risikoanalyser for terrorhendelser kan kommuniseres.** Problemstillingen er vanskelig fordi den ideelt sett skal gi svar på hvordan man kan kommunisere det man ikke vet. Det er lagt en kvalitativ metodisk tilnærming til grunn, hvor de empiriske funnene i all hovedsak baserer seg på dokumentanalyse. For å besvare spørsmålet i problemstillingen er det først valgt å belyse hvordan ulike tilnærminger til risiko kan forme forståelsen av terrorismerisikoen. Ved hjelp av teoretiske bidrag fra andre fagfelt, blant annet psykologi og atferdsteori, forsøkes det deretter å forklare hvilke elementer det er viktig å ta høyde for når terrorismerisikoen skal kommuniseres.

Studien konkluderer med at det er behov for en bayesiansk risikotilnærming sammen med en risikodefinitjon som tar høyde for usikkerhet. Risikotilnærmingen må anerkjenne opplevd risiko og bruk av subjektive/kunnskapsbaserte sannsynligheter. Dette er mest kompatibel med den dynamiske, komplekse og usikre terrorismerisikoen. I kommunikasjon av terrorismerisikoen er det avgjørende med en tydelig definisjon av begreper, ettersom særlig begrepene risiko, terrorisme og sannsynlighet har ulike tolkninger. Å formidle usikkerheten, selv om dette innebærer å si at man ikke vet, vurderes som å være den beste framgangsmåten. Da kan vi både ta høyde for tillit hos publikum og unngå å skape unødig frykt.

Summary

The threats facing Norway can be said to have changed, where the focus on intentional unwanted actions, particularly acts of terrorism, has increased. Events such as September 11, 2001, July 22, 2011 and the attack in In Amenas in 2013 have all changed our perception of risk and demonstrated that terrorist attacks can happen at home as well as target Norwegian interests abroad. The discussion concerning whether and how the risk of intentional actions can be controlled has been highlighted on the political and strategic level, in academia and in the media.

There is broad consensus that the large degree of uncertainty is what separates intentional unwanted actions (security), particularly the risk of terrorist acts, from accidental operation failures (safety). In this study the focus is on understanding risk management and risk communication and how these work in the context of terrorism. The main aim of the study is to answer the question of how to communicate the uncertainty of the risk of terrorist events. This issue is difficult, as it ideally should answer how to communicate something unknown. A qualitative approach is applied to answer the research questions, where the empirical findings are mainly based on document analysis. In order to answer the research questions, the first task is to illustrate how different approaches to risk can shape our understanding of terrorism risk. Then, by using theoretical contributions from other disciplines such as psychology and behavioral theory, the second task is to explain which elements should be taken into account when communicating the risk of terrorism.

The study concludes that a definition of risk that acknowledges uncertainty together with the Bayesian risk approach, which recognizes the perceived risk and the use of subjective/knowledge-based probabilities, is the most compatible with the dynamic, complex and uncertain case of terrorism risk. A clear definition of terms – particularly the terms risk, terrorism and probability have different interpretations – is considered crucial in the communication of terrorism risk. In order to avoid creating unnecessary fear and to account for the trust of the audience, the best practice is found to be to express the uncertainty, even if this means admitting that one does not know.

Innhold

Sammendrag	3
Summary	4
Forord	7
1 Innledning	9
1.1 Bakgrunn	10
1.2 Problemstilling	12
1.3 Avgrensning	13
1.4 Oppbygging	14
2 Kontekst	15
2.1 Relevante standarder og veiledere	15
2.2 Relevante aktører	16
2.3 Terminologi	18
3 Teori	19
3.1 Risiko	19
3.1.1 Ulike definisjoner på risiko	19
3.1.2 Tilsiktede uønskede handlinger og terrorisme	21
3.1.3 Terrorismerisiko	22
3.2 Ulike tilnærminger til risiko	22
3.3 Risikoanalyse	25
3.3.1 Sikringsrisikovurdering	25
3.3.2 Ekspertvurderinger og involvering av interessenter	26
3.3.3 Ulike metoder for risikoanalyse	28
3.4 Risikokommunikasjon	29
3.4.1 Kommunisere terrorismerisikoen	31
3.4.2 Risiko med høy usikkerhet	32
3.4.3 Framstillingsverktøy for risiko	33
4 Metode	37
4.1 Undersøkelsesdesign	37
4.2 Metodisk tilnærming	37

4.3	Forskningsstrategi	37
4.4	Datainnsamling	38
4.4.1	Samtaler med relevante aktører	38
4.4.2	Dokumentundersøkelser	39
4.4.3	Forholdet mellom metode, empiri og teori	39
4.5	Styrker og svakheter med designet	40
4.5.1	Reliabilitet	40
4.5.2	Validitet	40
5	Analyse	42
5.1	Relevante aktørers tilnærming til risiko	42
5.2	Risikoanalyse og involvering av interessenter	45
5.3	Sannsynlighetsdebatten i media	46
5.4	Usikkerhet	48
5.5	Kommunisere usikkerhet	48
5.5.1	Kommunisere usikkerhet i etterretning	49
5.5.2	Uttrykke usikkerhet med sannsynlighet	49
5.5.3	Eksempel på kommunikasjon av terrortrusselen fra PST	51
5.6	Sentrale elementer i kommunikasjon av risiko for terrorhandlinger	52
5.6.1	Tillit	52
5.6.2	Ord og tallforståelse	53
5.6.3	Risikopersepsjon og atferdsteori	54
6	Diskusjon	57
6.1	Risikoforståelse	57
6.1.1	Risikobegrepet i terrorismekontekst	57
6.1.2	Er terrorismerisikoen kompleks, usikker og tvetydig?	59
6.1.3	Risikotilnærming og kommunikasjon av terrorismerisiko	60
6.2	Risikoanalyse: samme formål og ulike resultater?	64
6.3	Kan terrorismerisikoen framstilles visuelt?	65
6.4	Kommunisere risiko uten å bidra til unødig frykt	67
6.5	Hvordan kan vi kommunisere det vi ikke vet?	69
7	Konklusjon	72
	Forslag til videre forskning	74
	Referanser	75

Forord

Denne rapporten er skrevet med min masteroppgave i samfunnssikkerhet fra Universitetet i Stavanger som utgangspunkt. Det er gjort noen endringer for å tilpasse den rapportmalen, men funnene er de samme. I forbindelse med studien er det flere som må takkes. Først og fremst vil jeg takk min veileder Tonje Grunnan for et kritisk blikk, motiverende ord og stødig veiledning gjennom hele prosessen. En nærmest like stor takk fortjener Forsvarets forskningsinstitutt, og særlig prosjektgruppa Beskyttelse av samfunnet, for å ha tatt godt i mot meg og gitt meg mulighet til å skrive masteroppgaven i samarbeid med dem. Takk til Maren Maal for gode diskusjoner, og takk til Monica Endregard for konstruktive tilbakemeldinger. Sissel Haugdal Jore ved Universitetet i Stavanger må også takkes for gode diskusjoner i startfasen og oppklarende svar i slutfasen.

Jeg vil også takke Ann Karin Midtgård ved Direktoratet for samfunnssikkerhet og beredskap og Jon Fitje Hoffmann ved Politiets sikkerhetstjeneste for å ha satt av tid til å snakke med meg.

Kjeller, 22.mars 2017

Janita Andreassen Bruvoll



1 Innledning

«There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. There are things we don't know we don't know» (Donald Rumsfeld, 2002).

Samfunnssikkerhet er et relativt nytt fagfelt, men har i løpet av de siste tiårene blitt mer og mer relevant og omfattende. Hva som skal inngå, og hvilke hendelser som er relevante for samfunnssikkerhet har vært omdiskutert. I NOU 'en "Når sikkerhet er viktigst" (JD, 2006) uttales det at samfunnssikkerhet har gått fra å omhandle ekstraordinære hendelser til å legge forebygging av uønskede hendelser til grunn. Disse hendelsene inkluderer naturskapt og menneskeskapt hendelser, både utilsiktede hendelser og tilsiktede handlinger.

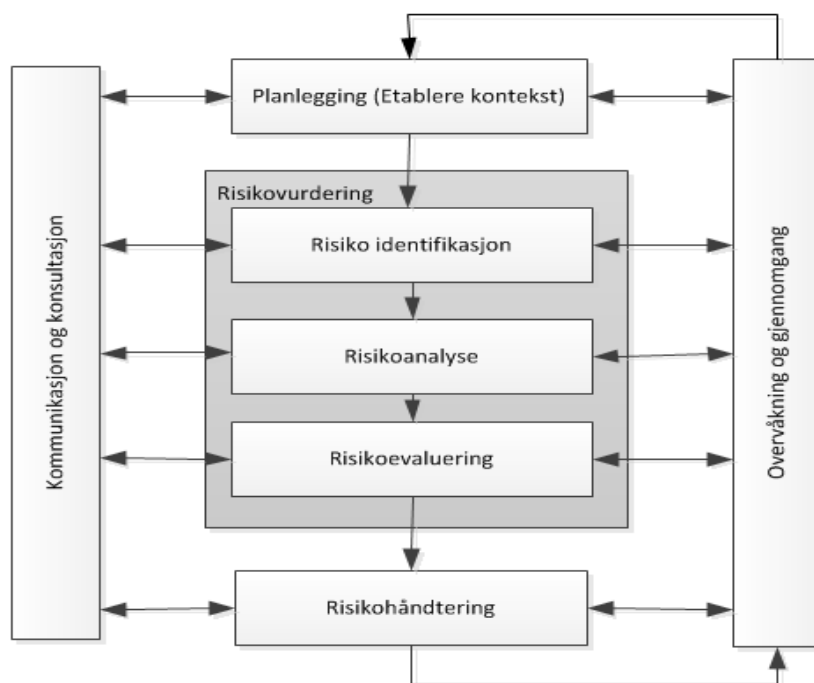
Denne studien avgrensers seg til å omhandle tilsiktede handlinger, og da med særlig fokus på terrorhendelser. Hensikten med studien er å se nærmere på risikoforståelse og risikokommunikasjon i en terrorismekontekst. Risikoforståelsen er avgjørende for hvordan man både vurderer, håndterer og styrer risiko, og formålet i denne oppgaven vil være å se hvordan ulike tilnærminger til risiko former forståelsen av terrorismerisikoen, og også legger føringer for hvordan man kommuniserer terrorismerisikoen. Kommunikasjon av terrorismerisikoen handler i stor grad om å kommunisere usikkerhet, altså det man ikke vet, og det vil da være avgjørende at den risikotilnærmingen som ligger til grunn for vurderingene faktisk erkjenner og legger føringer for håndtering av usikkerhet.

Terrorfenomenet har vært en aktualitet i flere århundrer, men det kan sies å ha endret karakter og fått økt oppmerksomhet, både hos myndighetene, media og befolkningen, siden starten på 1990-tallet. Terrorangrepet i New York 11. september 2001 endret, i følge Jore (2012), vår persepsjon omkring risikoen for tilsiktede handlinger, og flere verdensomspennende sikringstiltak, som økt sikkerhetskontroll på flyplasser, ble iverksatt. Bombeangrepet og skytingen 22. juli 2011 og angrepet mot gassinstallasjon i In Amenas i 2013 har vist at terrorhendelser også kan ramme oss her hjemme samt norske interesser i utlandet. Disse hendelsene, og granskningen i etterkant, har satt mange viktige saker på den politiske og strategiske agendaen. Både Gjørsv-kommisjonens 22.juli-rapport og Statoils granskningsrapport etter In Amenas konkluderer med at det ikke har vært tilstrekkelig med fokus på forebygging av tilsiktede handlinger (NOU, 2012:14 og Statoil, 2013). Selv om disse hendelsene har skapt økt fokus samt økt engasjement og vilje til å forbedre vår håndtering av risikoen relatert til terrorhendelser, virker det fortsatt å være flere kunnskapshull. Justis- og beredskapsdepartementet (JD) uttaler i sin FoU-strategi, gjeldende fra 2015-2019, at det er et kunnskapsbehov innen blant annet risikoforståelse, risikoerkjennelse og forbygging av terrorisme (JD, 2015a og JD, 2015b).

1.1 Bakgrunn

Den tyske sosiologen Ulrich Beck skrev: “Neither science, nor the politics in power, nor the mass media, nor the law nor even the military are in a position to define or control risk rationally” (Beck, 2006:336). Han introduserte oss for begrepet risikosamfunnet, som innebærer at det finnes grenseløse risikoer som ikke kan kontrolleres gjennom teknologiske inngrep, uansett hvor mye vi forsøker. Beck (2006) definerer moderne terrorisme som en trussel vi ikke kan kontrollere. Både før, og særlig etter, Beck introduserte oss for risikosamfunnet som begrep har temaet om hvorvidt ulike risikoer kan styres vært omdiskutert. Dette har gjort seg særlig gjeldende innenfor risiko tilknyttet tilsiktede uønskede handlinger.

Risikostyring kan defineres som ”... en kontinuerlig ledelsesprosess som har som målsetning å identifisere, analysere og vurdere mulige risikoforhold i et system eller i en virksomhet, samt å finne fram til og iverksette tiltak som kan redusere mulige skadevirkninger” (Rausand og Utne, 2009:369). Aven (2015:13) hevder at risikostyringsprosessen på den ene siden dreier seg om å få innsikt i risikoforhold, effekt av tiltak, grad av styrbarhet av risiko osv., mens det på den andre siden handler om metoder, prosesser og strategier for å kunne kartlegge og styre risikoene. Risikostyring anses som en prosess som foregår kontinuerlig, hvor formålet er “å sikre den riktige balansen mellom det å utvikle og skape verdier, og det å unngå ulykker, skader og tap” (Aven, 2015:14). Forbindelsen og rekkefølgen av risikostyringsprosessen kan best oppsummeres med en figur:



Figur 1.1 Risikostyringsprosessen (Aven, 2015:15).

Forskjellen på safety og security

De engelske begrepene safety og security benyttes ofte for å skille mellom de ulike aspektene ved sikkerhet. På norsk oversetter vi gjerne begrepene til trygghet (safety) og sikkerhet (security). Trygghet refererer til å være beskyttet, mens sikkerhet betyr å være uten fare. Med disse definisjonene til grunn er det mer nærliggende å tenke at den ene fører til den andre, men det gir ikke en umiddelbar forståelse av forskjellen (Albrechtsen, 2003). Rausand og Utne (2009) forklarer skillet ved å beskrive safety som sikkerhet mot tilfeldige hendelser som naturhendelser og teknisk svikt, mens security er sikkerhet mot vilde eller intenderte handlinger, som sabotasje, spionasje og terror. Albrechtsen (2003) gjør en mer omfattende analyse av begrepene og hevder det finnes langt mindre forskning på styring av risiko tilknyttet security-relaterte risikoer enn for safety-relaterte risikoer. Samtidig poengterer han at security-feltet har mye å lære av safety-feltet. De viktigste forskjellene mellom safety og security, i følge Albrechtsen (2003), er beskrevet i figuren under.

	Security	Safety
Causes	An incident is most often a result of one person or a group's will	An incident is most often a result of human behaviour in combination with the environment
Causes	Often planned actions	Often unplanned
Causes	Criminal acts	Criminal acts (Working Environment Act)
Causes	Mainly malicious acts	Seldom, if ever, malicious
Causes	Mainly deliberate acts with a wish of a wanted output/consequence of the act.	Mainly deliberate acts without a wish of a wanted output and accidental incidents
Threats/hazards	External and internal human threats	Internal human threats
Threats/hazards	Threats are not always observable, tangible and proximate	Hazards are observable, tangible and proximate
Loss	Loss is mainly related to physical assets and information	Loss is related to human injuries/death and reliability of industrial assets
Surroundings	Reflects the state of society through its structures, economical situation, law-abidingness and moral	Includes physical and environmental conditions – not only humans and society
Relevance	Relevant for a wide range of companies	More relevant for the industry and transporting sector
Uncertainty	High degree of <i>uncertainty</i> and low degree of knowledge about threats within	

Figur 1.2 Forskjellene mellom safety og security (Albrechtsen, 2003:13).

Det er ikke bare de semantiske utfordringene som har vært gjeldende innenfor security-feltet; diskusjonen om hvorvidt man kan vurdere risikoen for tilsiktede handlinger med samme metoder og verktøy som risikoer knyttet til utilsiktede hendelser har lenge vært aktuell. Debatten rundt hvorvidt en skal benytte sannsynlighet for tilsiktede handlinger har også vært

framtreddende. Den grunnleggende forståelsen og tilnærmingen til risiko vil være med på å prege hva som ligger til grunn for sannsynlighetsvurderingen. Tradisjonelt sett er risiko sett på som en kombinasjon eller en funksjon av konsekvens og sannsynlighet, og en har fastsatt sannsynligheter ved hjelp av en frekvensbasert tilnærming. Dette betyr at vi ut ifra tidligere hendelser har forsøkt å predikere fremtiden. For tilsiktede hendelser anses dette som en utfordrende og lite hensiktsmessig framgangsmåte; vi har få, eller ingen, tidligere hendelser å vise til, og andre faktorer blir da nødvendig å inkludere for å få en realistisk vurdering av det gjeldende risikobildet. For tilsiktede handlinger, og risiko generelt, er det blitt vanlig å referere til en kunnskapsbasert eller subjektiv sannsynlighet. Dette innebærer at flere faktorer blir vurdert, og framfor kun å kombinere sannsynlighet og konsekvens tar vi med usikkerheten knyttet til begge, og estimerer en sannsynlighet gitt den kunnskapen man innehar på gitt tidspunkt. Den sistnevnte måten å se på risiko fordrer ikke nødvendigvis nye analysemetoder, men et større behov for å kommunisere hva som ligger til grunn for risikovurderingen da den ikke baserer seg på statistikk og tidligere hendelser.

1.2 Problemstilling

Forsvarets forskningsinstitutt (FFI) leverte i juni 2015, på oppdrag fra Forsvarsbygg, en rapport som hadde som formål å vurdere tilnærminger til risikovurderinger for tilsiktede uønskede handlinger (Busmundrud, Maal, Kiran og Endregard, 2015). Her vurderte FFI Forsvarsbyggs operasjonalisering av de to norske standardene, NS 5814:2008 og NS 5832:2014, som Forsvarsbygg benytter i sine risikovurderinger av tilsiktede handlinger. Formålet var å se om de burde vurdere å få inn nye momenter eller forbedre sine eksisterende modeller.

Gjennomgangen av de to tilnærmingene, som Forsvarsbygg bruker, viste at felles for begge var en systematisk framgangsmåte hvor en identifiserer verdier knyttet til objektet som undersøkes samt trusler og sårbarheter/konsekvenser. Busmundrud et al. (2015) mener begge standardene ser ut til å legge føringer for bruk av sannsynlighet, men mens NS 5814:2008 uttrykker dette eksplisitt framkommer det i NS 5832: 2014 som en implisitt oppfordring. Når man snakker om sannsynlighet i forbindelse med risikovurderinger for tilsiktede handlinger henvises det til bruk av en kunnskapsbasert/subjektiv sannsynlighet, framfor den tradisjonelle frekvensbaserte og matematiske sannsynligheten. Dette skillet uttrykkes eksplisitt i NS 5814:2008, hvor det gjøres et skille mellom en kvantitativ og en kvalitativ tilnærming til sannsynlighet, hvor den sistnevnte refererer til et uttrykk for *muligheten* for at en hendelse skal inntreffe. I NS 583X-serier brukes ikke sannsynlighetsbegrepet.

Manglende fokus på bruk av sannsynlighet er uheldig; blant annet kan dette skape forvirring omkring hvorvidt sannsynligheten en setter for en tilsiktet handling skal forstås som en objektiv sannhet eller en subjektiv vurdering basert på den kunnskapen og informasjon en innehar på et gitt tidspunkt. Videre fordrer begge tilnærmingene til sannsynlighet at usikkerheten som ligger til grunn blir kommunisert, og da for kunnskapsbasert sannsynlighet i større grad enn frekvensbasert sannsynlighet. *Begge tilnærmingene får i FFI-rapporten kritikk for ikke å legge noen føringer for hvordan en skal kommunisere usikkerheten som ligger til grunn for*

risikovurderingene. NS 5832: 2014 får i tillegg kritikk fra Busmundrud et al. (2015) og flere av informantene i rapporten for ikke å ha tilstrekkelig vitenskapelig forankring.

For å kunne vurdere, håndtere og kommunisere risiko er man avhengig av å ha forståelse for hva risiko er. Blant andre Aven (2007, 2015), Renn (2008), NSM (2016), Engen og Pettersen (2010) og Jore og Njå (2010) hevder at tilnærmingen og forståelsen av risiko er avgjørende for hvordan den styres. Målet for denne oppgaven er derfor å først redegjøre for hvilken betydning ulike risikotilnærminger har for risikoforståelsen, og da i en terrorismekontekst. Deretter vil fokuset rettes mot risikokommunikasjon, og da med vekt på usikkerheten tilknyttet risikoen for terrorhendelser.

Risikovurderinger handler tradisjonelt om noe man gjør i nåtid, basert på fortiden med mål om å kunne si noe om fremtiden. Fremtiden er usikker, og uansett hvor mange risikoanalyser som gjennomføres vil man aldri med 100 % sikkerhet kunne si noe om hvilke hendelser som vil skje, hvilke konsekvenser de vil medføre og når de vil inntreffe. Målet må derfor være å få et best mulig beslutningsgrunnlag, basert på den tilgjengelige informasjonen man har, og dermed, om mulig, forebygge og dimensjonere sikkerhetstiltak. Når denne informasjonen skal formidles er det viktig at man samtidig som å uttrykke det man vet, også formidler det man ikke vet for å skape et mest mulig korrekt bilde av situasjonen.

Siden terrorhendelser skiller seg fra andre hendelser ved at de er preget av stor grad av usikkerhet og ulike forståelser av hvordan man på best måte kan vurdere og tilnærme seg risikoen ledet dette til problemstillingen:

Hvordan kan man kommunisere usikkerheten i risikoanalyser for terrorhendelser?

For å besvare problemstillingen deles den opp i to forskningsspørsmål.

Hvordan påvirker ulike tilnærminger til risiko forståelsen og vurderingen av terrorisimerisikoen?

Hvilke elementer vil være viktig å inkludere i kommunikasjonen av resultatene fra risikoanalyser for terrorhendelser?

1.3 Avgrensning

Denne rapporten er avgrenset til å omhandle tilsiktede uønskede handlinger, hvor særlig terrorhendelser er vektlagt. Når det gjelder risikoforståelse er det valgt å benytte nasjonale offentlige aktører som eksempel, hvor PST og DSB er vurdert som de mest relevante. NSM er også tatt med da de også har som oppgave å vurdere tilsiktede uønskede handlinger, samt at de har bidratt betraktelig i forbindelse med operasjonalisering av trefaktortilnærmingen i veileder og egen håndbok.

I oppgaven er det valgt å se på risikoforståelse ut fra teknisk/naturvitenskapelig-, bayesiansk- og trefaktortilnærmingen til risiko. Når det gjelder kommunikasjon er det valgt å avgrense seg til risikokommunikasjon, som betyr at det i all hovedsak vil omhandle kommunikasjon som foregår før en hendelse inntreffer. Som vist i figur 1.1 er kommunikasjon indentifisert som et viktig element i alle delene av risikostyringsprosessen. I denne oppgaven vil det være fokus på kommunikasjon av resultatene fra risikoanalysen. Det er kommunikasjon mellom analytikerne og beslutningstakerne som er utgangspunktet for denne oppgaven. En utfordring her er at de fleste risikovurderinger for tilsiktede uønskede handlinger, og særlig terrorhandling, er graderte, og de fleste eksemplene som finnes er hvor myndighetene kommuniserer informasjon ut til befolkningen. Det er derfor også blitt inkludert i oppgaven, og hovedvekten er lagt på elementer som usikkerhet, tillit, risikopersepsjon, atferdsteori og ord- og tallforståelse, som må kunne sies å være relevant i kommunikasjon både til beslutningstakere og befolkningen. Utfordringen i forbindelse med gradert utilgjengelig informasjon gjør også at oppgaven fokuserer på forutsetningen for å lykkes med risikokommunikasjon, og mindre på selve innholdet som formidles. Håndtering av terrorhendelser vil falle utenfor rammene til denne studien. En annen avgrensning med studien er at den baserer seg på teoretiske betraktninger framfor praktisk erfaring. Dette valget er også tatt på bakgrunn av manglende tilgang og mulighet til å formidle informasjon av en slik art. Det er derfor også viktig å påpeke at resultatene kunne vært annerledes om kunnskapsgrunnlaget også hadde inkludert det praktiske aspektet.

1.4 Oppbygging

Denne rapporten er delt inn i 7 kapitler. Etter innledningskapitlet med beskrivelse av problemstillingen og avgrensning presenteres relevante standarder og aktører i kontekstkapitlet. Deretter presenteres oppgavens teoretiske rammeverk i kapittel 3. I kapittel 4 beskrives den metodiske tilnærmingen, hvor det er vektlagt å redegjøre for valg og framgangsmåte. Analysekapitlet presenterer oppgavens empiriske grunnlag, hvor teorikapitlet er lagt til grunn for kapitlets struktur. I kapittel 6 diskuteres de empiriske funnene opp mot det teoretiske rammeverket før det i kapittel 7 redegjøres for konklusjoner. Helt til sist kommer det noen forslag til videre forskning.

2 Kontekst

I denne oppgaven er det referert til ulike standarder for risikostyring og -vurdering. Disse standardene vil ikke bli analysert eller diskutert i sin helhet, men de er benyttet for å se hvordan ulike begreper og framstillingsverktøy er definert og operasjonalisert. Første del av kapitlet vil gi en kort beskrivelse over hva som inngår i standardene, og så vil ulike begreper bli presentert i en oppsummerende tabell. Andre del av kapitlet gir en beskrivelse av de ulike aktørene som er relevant for denne oppgaven. Avslutningsvis presenteres en terminologiliste.

2.1 Relevante standarder og veiledere

NS-ISO 31000 Risikostyring – Prinsipper og retningslinjer

Denne standarden retter seg mot organisasjoner av alle størrelser og typer som har behov for å håndtere risiko. I standarden blir det både presentert og beskrevet prinsipper, rammeverk og en prosess som skal kunne håndtere en hver form for risiko. Den skal også være behjelpelig med å hjelpe organisasjonen til å utvikle sin egen tilnærming til risiko (NS-ISO 31000:2009).

NS 5814 Krav til risikovurderinger

Denne standarden baserer seg i stor grad på ISO 31000, men fokuserer på risikovurderinger og de elementene som bør inngå i denne prosessen. Standarden er generell og retter seg mot fag, bransjer og næringer som ikke har egne standarder for risikovurderinger (NS 5814:2008).

NS 5830 Beskyttelse mot tilsiktede uønskede handlinger – Terminologi

Standarden gir en innføring i begreper innenfor fagområdet sikring (NS 5830:2012).

NS 5832 Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse.

Standarden retter seg mot sikkerhetsanalytikere og beslutningstakere for virksomheter som har behov for sikkerhetsanalyse/vurdering. Den skal være gjeldende for både statlige, kommunale og private virksomheter. Denne standarden er avgrenset til å omhandle tilsiktede uønskede handlinger, som ran, tyveri, terror og vandalisme (NS 5832:2014).

Terrorsikring – En veileder i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger

Veilederen retter seg mot offentlige og private virksomheter som et hjelpemiddel for å planlegge og iverksette sikringstiltak mot terrorhandlinger. Veilederen er i samsvar med NS 583X-serien (NSM, POD og PST, 2015).

Håndbok for risikovurdering for sikring

Håndboken beskriver hvordan risikovurderinger av tilsiktede uønskede handlinger kan planlegges, gjennomføres og dokumenteres. Den retter seg mot alle virksomheter, og hensikten er å øke sikkerhetsbevisstheten i virksomhetene. Håndboken baserer seg på rammeverket NS 5832 (NSM, 2016).

Tabell 2.1 Oversikt over relevante standarder.

Standarder og veiledere	Risikobegrepet	Risikovurdering	Risikoanalyse	Safety/security
ISO 31000	Uttrykk for kombinasjonen av sannsynlighet og konsekvensen av en uønsket hendelse.	Risikoanalyse+ risikoevaluering	Systematisk framgangsmåte for å beskrive og/eller beregne potensielt tap (risiko) gjennom kartlegging av uønskede hendelser, og årsaker til og konsekvensene av disse.	Ja/ja
NS 5814				Ja/ja
NS 583X ¹	Uttrykk for forholdet mellom trusselen mot en gitt verdi og denne verdien sårbarhet overfor den spesifiserte trusselen.	Helhetsvurdering basert på verddivurdering (eller konsekvensvurdering), trusselvurdering og sårbarhetsvurdering med mål om å angi en entitets ² risiko i en definert sikringsmessig kontekst.	Sikringsrisikovurdering samt vurdering av strategi og tiltak.	Nei/ja
Veileder Terrorsikring (NSM, POD og PST)				Nei/ja
Håndbok risikovurdering sikring (NSM)				Nei ³ /ja

2.2 Relevante aktører

Politiets sikkerhetstjeneste (PST)

PST er underlagt Justis- og beredskapsdepartementet (JD) og er trolig Norges viktigste aktør innenfor forebygging av terrorisme. Deres primære ansvar er “å forebygge og etterforske straffbare handlinger mot rikets sikkerhet. Dette gjør tjenesten gjennom ulike metoder og arbeidsmåter. Sentralt står innsamling av informasjon om personer og grupper som kan utgjøre en trussel, utarbeidelse av ulike analyser og trusselvurderinger, etterforskning og andre

¹ Brukes som et samlebegrep for NS 5830, NS 5831 og NS 5832.

² Fysisk objekt, individ, organisasjon, stat, gruppering, virksomhet eller annen enhet som passer inn i sammenhengen (NS 5832:2014, s. 4).

³ Innledningsvis utelukker ikke NSM bruk av håndboken for tilsiktede hendelser, men det er ingen videre beskrivelse av hvordan dette skal utføres.

operative tiltak og rådgivning” (PST.no). PST gir årlig ut en åpen trusselvurdering, og gjennomfører ikke helhetlige risikovurderinger.

Nasjonal sikkerhetsmyndighet (NSM)

NSM er underlagt Forsvarsdepartementet (FD) og JD og er Norges ekspertorgan for informasjons- og objektsikkerhet, og det nasjonale fagmiljøet for IKT-sikkerhet (nsm.no). De har blant annet som oppgave å vurdere risiko innen forebyggende sikkerhet og foreslå sikkerhetsfremmende tiltak (NSM, 2016b) NSM leverer også ukentlige sikkerhetsanalyser til blant andre JD og FD.

Direktoratet for samfunnssikkerhet og beredskap (DSB)

DSB er underlagt JD og skal ha oversikt over risiko og farer i samfunnet. Direktoratet skal være pådriver i arbeidet med å forebygge ulykker, kriser og andre uønskede handlinger, samt sørge for god beredskap og effektiv ulykke- og krisehåndtering (DSB, 2012). DSB har siden 2011 gitt ut årlig nasjonalt risikobilde (NRB). Her beskrives alvorlige krisescenarioer og alvorlige risikoforhold. I forbindelse med utgivelse av NRB er også DSB den av de undersøkte aktørene som best har redegjort for sin risikoforståelse, både i NRB-rapporten (2014) og i et separat metodedokument (DSB, 2015).

2.3 Terminologi

Tabell 2.2 Relevante begreper for oppgaven.

Terminologi	
Safety	Sikkerhet mot uønskede hendelser som resultat av tilfeldigheter (NOU, 2006:6, s. 38)
Security	Sikkerhet mot uønskede hendelser som resultat av overlegg (NOU, 2006:6, s. 38)
Risiko	Risiko referer til usikkerheten om alvorlighetsgraden til en hendelse og konsekvensene tilknyttet en aktivitet i forbindelse med noe mennesker verdsetter (Aven og Renn, 2010:3).
Sikringsrisiko	Forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet over den spesifikke trusselen (NS 5832, 2014:4)
Usikkerhet	Usikkerhet er differansen mellom den informasjonen som er nødvendig for å ta en sikker beslutning og den informasjonen som er tilgjengelig på tidspunktet for beslutningen (Norsk senter for prosjektledelse).
Trussel	Mulig uønsket handling som kan gi negativ konsekvens for en entitets sikkerhet (NS 5830:2012, s. 4)
Verdi	Ressurs som hvis den blir utsatt for uønsket påvirkning vil medføre en negativ konsekvens for den som eier, forvalter eller drar fordel av ressursen (NS 5830:2012, s. 4)
Sårbarhet	Manglende evne til å motstå en uønsket hendelse eller å opprette ny stabil tilstand dersom en verdi er utsatt for uønsket påvirkning (NS 5830:2012, s. 5)
Risikokommunikasjon	En interaktiv prosess med informasjon og oppfatning blant enkeltpersoner, grupper og institusjoner. Dette innebærer flere meldinger som omhandler selve risikoen, men også andre meldinger, som strengt tatt ikke er om risiko, men som uttrykker bekymringer, meninger eller reaksjoner tilknyttet risikomeldinger eller til juridiske og institusjonelle ordninger for risikostyring (Aven og Renn 2010:159).

3 Teori

I dette kapitlet blir det teoretiske rammeverket som er relevant for å belyse problemstillingen presentert. Teorien blir presentert i en rekkefølge som er med på å strukturere analysen og sammenhenger i diskusjonen. Først vil ulike definisjoner av og tilnæringer til risiko bli presentert. Deretter blir risikoanalyse og ulike verktøy som er relevante for oppgaven presenteres. Til slutt blir teori om risikokommunikasjon og usikkerhet redegjort for.

3.1 Risiko

Det finnes ikke én felles akseptert definisjon av risiko, og når en studerer litteraturen som omhandler risiko finner en at risiko både ses på som en forventet verdi, som en sannsynlighetsfordeling, som usikkerhet og som en hendelse (Aven og Renn, 2010). Begrepet risiko blir i dag brukt i mange ulike sammenhenger og har, som nevnt ovenfor, forskjellig og ofte uklar betydning. I følge Aven, Boyesen, Njå, Olsen og Sandve (2004) er oppfatningen og forståelsen en har om risiko viktig og har videre betydning for hvordan en handler for å styre sikkerhet og risiko. Risiko handler om framtiden, men det benyttes gjerne tidligere hendelser og ervervet kunnskap for å kunne predikere framtidig risiko. På denne måten ser man sammenhenger og finner forklaringer i hendelser som har skjedd for å kunne forstå hvilke risikoer som er relevante i framtiden. Gjennom risikoanalyser forsøker analytikere å samle informasjon og kunnskap om objektene, systemene og/eller verdiene som undersøkes, og benytter denne informasjonen for å si noe om den tilhørende usikkerheten. Et viktig element å vektlegge her er at dette blir en vurdering sett gjennom noens øyne, og hva som velges å fokusere på vil ikke alltid være opplagt eller det samme for ulike grupper med analytikere. Dermed blir risiko avhengig av både hvem som vurderer og hva som vurderes (Aven et al., 2004).

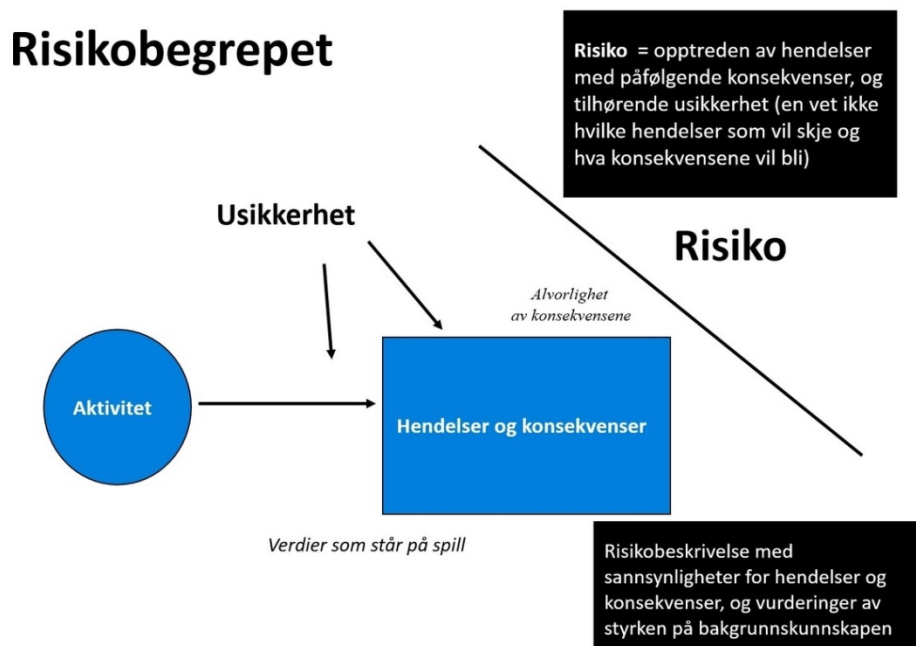
De fleste definisjonene av begrepet risiko, har i følge Ortwin Renn (2008), ett felles element: Skillet mellom mulig og valgt handling: *"Til en hver tid står et individ, en organisasjon eller et samfunn over flere valg i forbindelse med en handling (inkludert å ikke gjøre noe), hvor hvert valg er assosiert med potensielle positive og negative konsekvenser"* (Renn, 2008:1). Noen ganger kan en beslutning reverseres om konsekvensene blir verre enn forventet og en kan gå tilbake til beslutningssituasjonen, men det vil aldri være mulig å starte helt forfra.

3.1.1 Ulike definisjoner på risiko

Aven (2012a) gir en historisk framstilling av hvordan risikobegrepet er brukt og definert fra det 12. århundre til i dag. Han hevder det at det er mulig å finne interessante aspekter ved risikobegrepet ved å undersøke tidsdimensjonen. Det å studere det historiske aspektet kan både lede til en bredere forståelse av risikostyringsprosessen og kan også gi oss en oppfatning om vi beveger oss i riktig retning innenfor feltet. Aven (2012a) utelukker risikodefinitjoner som kun tar høyde for forventet tap og rene sannsynlighetsbaserte perspektiv da disse ikke tar tilstrekkelig høyde for usikkerhet. Risiko er som oftest knyttet til noe skadelig eller ubehagelig

og for denne oppgaven vil risiko bli sett på som noe negativt, og det positive aspektet med at man potensielt kan tjene noe på en aktivitet er ikke vurdert som hensiktsmessig å inkludere.

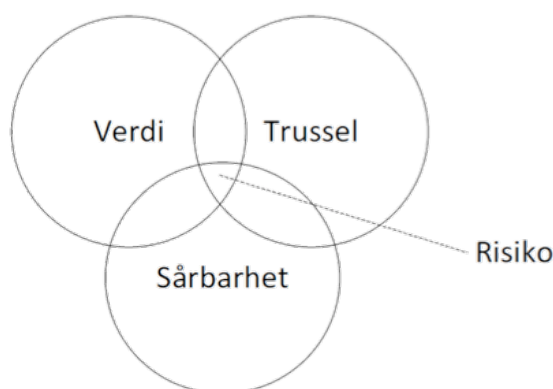
Risiko har tradisjonelt vært sett på som en kombinasjon av sannsynlighet for at en hendelse kan inntreffe og konsekvensene de medfører. Det er ingen tvil om at disse faktorene fortsatt spiller en viktig rolle, og at variablene har en sentral rolle i både analyseringen, evalueringen og kommunikasjon av risiko. Aven og Renn (2010) mener at vi i dag har behov for et bredere perspektiv på risiko, og har i sin risikodefinesjon gitt usikkerhet større oppmerksomhet: *”Risk refers to uncertainty about and severity of the consequences (or outcomes) of an activity with respect to something that humans value”* (se figur 3.1) (Aven og Renn, 2010:3). I forbindelse med risiko i en security-kontekst, vil da risikoen referere til usikkerheten tilknyttet konsekvensene og alvorlighetsgraden av et eventuelt angrep. De anbefaler videre at risikoen beskrives og at usikkerhet uttrykkes. Måten å uttrykke usikkerheten kan, i følge Aven (2015), gjøres via subjektive eller kunnskapsbaserte sannsynligheter, gitt at en redegjør for bakgrunnsinformasjonen som ligger til grunn for sannsynlighetsvurderingen. Her ser vi at sannsynlighetsbegrepet ikke er en del av definisjonen, men implisitt i definisjonen ligger sannsynlighet som et verktøy for å uttrykke deler av resultatet.



Figur 3.1 Risikodefinesjon (Aven og Renn, 2010)

NS 5830:2012, “Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi”, en del av NS 5830-serien, ble utgitt som et anbefalt rammeverk spesielt for sikringsrisikostyring. Her defineres risiko som: *“forholdet mellom trusselen mot en gitt verdi og denne verdiens sårbarhet over den spesifikke trusselen”*, og betegnes som trefaktormodellen (se figur 3.2). I denne definisjonen er sannsynlighetsbegrepet utelatt, og seksjonsleder i PST Bård Olsen (2012), poengterer at det er bevisst at både konsekvens- og sannsynlighetsbegrepet ikke

brukes. Begrunnelsen er at terror forekommer så sjeldent at det er lite empiri å bygge på, og at det dermed ikke kan beregnes hyppighet eller forekomst av slike lavfrekvensfenomener ut fra historiske data, statistikk eller andre erfaringer. ”Ren risiko”, av det engelske begrepet ”pure risk”, er innført som begrep for å avgrense det til at konsekvensene av en hendelse kun kan medføre tap, og ingen gevinst (NS 5832:2014). ”Ren risiko” er opprinnelig kjent fra økonomifeltet og referer til en risiko hvor tap er det eneste mulige utfallet (investopedia a). Begrepet står i motsetning til ”spekulativ risiko” som betyr at det er usikkert hvorvidt resultatet vil være tap eller gevinst (investopedia, b).



Figur 3.2 Risikodefinsjon NS 538X-serien

3.1.2 Tilsiktede uønskede handlinger og terrorisme

En tilsiktet uønsket handling, eller en intendert hendelse, defineres av Norsk Standard (NS) 5830:2012 (s.2), som *en hendelse som forårsakes av en aktør som handler med hensikt*. Aktørens hensikt kan være ondsinnet eller å fremme egne interesser (DSB, 2014). Årsaken til slike hendelser vil ofte ligge i et komplekst samspill mellom teknologiske, organisatoriske og menneskelige faktorer, og årsakene kan sies å være knyttet til motivene til de som står bak (Aven et al., 2004).

Terrorisme er et begrep som de fleste av oss leser eller hører om daglig, både i nyhetsbildet og via sosiale medier, og begrepet brukes i et bredt spekter. Det benyttes for handlinger som bombing av bygninger, henrettelse av mennesker, forgiftning og forurensning. I følge Hoffman (2006) er terrorisme et begrep som de fleste har en vag forståelse av, men at en mangler en presis, konkret og virkelig beskrivende definisjon av begrepet. Han kritiserer en rekke definisjoner for å være lite tilfredsstillende, men peker på Oxford English Dictionarys (OED) definisjon av ”terrorist” som mer avklarende:

A political term: a. Applied to the Jacobins and their agents and partisans in the French Revolution, esp. to those connected with the Revolutionary tribunals during “Reign of Terror”, b. Any one who attempts to further his views by a system of coercive intimidation; *spec*, applied to members of one of the extreme revolutionary societies in Russia (Hoffman, 2006:2).

Hoffman (2006) hevder denne definisjonen er hjelpsom fordi at den, for det første, introduserer leseren for det faktum at terrorisme er et politisk konsept. Dette mener han er helt avgjørende for forståelsen av terroristens motivasjon, mål og formål, og er kritisk for å kunne skille terrorisme fra andre typer voldshandlinger. Videre hevder han at i den mest aksepterte og moderne bruken av begrepet, er det politiske aspektet fundamentalt og iboende. I tillegg handler det om streben etter, og bruk av makt for å oppnå politisk endring. OED har utvidet definisjonen av "terrorist" med følgende: "*Any one who attempts to further his views by a system of coercive intimidation*". Dette er, i følge Hoffman, med på å vise det andre fundamentale kjennetegnet med terrorisme; at det er en planlagt, kalkulert og systematisk handling (Hoffman, 2006).

For tilsiktede handlinger, som terrorangrep, finner man usikkerhet- og kunnskapsdimensjonen langt mer dynamisk enn for safety-relaterte hendelser. En hendelse som skjer på andre siden av jorda kan raskt endre risikovurderinger for terrorhendelser her hjemme, sannsynligheter så vel som styrken av kunnskapsgrunnlaget; det samme gjelder for overvåkning- og etterretningsarbeid (Aven, 2014).

3.1.3 Terrorismerisiko

Det har til nå blitt redegjort for ulike definisjoner av risiko og beskrivelsen viser at det legges ulik betydning i samme begrep. I denne oppgaven er ett av målene å se hvordan ulike forståelser av risiko kan påvirke oppfattelsen av risikoen relatert til terrorhendelser. Terrorismerisiko er ikke et anerkjent begrep på norsk, men *terrorism risk* benyttes ofte på engelsk. Det er i denne oppgaven valgt å benytte begrepet terrorismerisiko da både risiko og sikringsrisiko allerede er befestet med ulike forståelser. I begrepet ligger da usikkerheten knyttet til, og de negative konsekvensene av, en potensiell terrorhendelse.

3.2 Ulike tilnæringer til risiko

Tilnærmingen til risiko referer til forståelsen og oppfatningen man har til risiko. Viktigheten med å understreke at det finnes ulike syn på risiko er at de ulike forståelsene av risiko legger føringer for hvordan vi både studerer, vurderer og håndterer risiko. I dette delkapitlet vil det redegjøres for fire ulike tilnæringer til risiko.

Teknisk-naturvitenskapelig tilnærming til risiko

Innen teknisk-naturvitenskapelig tilnærming har fokuset vært på beregning og analyse av risiko ved bruk av matematiske og fysiske modeller (Aven et al., 2004:38). Ved en slik tilnærming uttrykkes ofte risiko kvantitativt i form av tall. Tilnærmingen bygger på en naturvitenskapelig tenkemåte hvor analytikeren på bakgrunn av tidligere hendelser forsøker å estimere sannsynligheter for risiko for framtiden. Innebygd i denne tenkingen er forståelsen om at risiko og sannsynlighet er objektive størrelser, som for eksempel høyde og vekt. Problemet her blir imidlertid at det ofte er langt vanskeligere å få like nøyaktige målinger på risiko og sannsynlighet, som for høyde og vekt, og konsekvensene blir da at estimatene blir usikre. Hampel (2006) hevder at fordelene med å vurdere risiko ut fra parameterne sannsynlighet og konsekvens er at det gir mulighet til å sammenligne risikoer. En forutsetning for at dette skal

kunne skje er at det er konsensus om hvordan sannsynlighet og konsekvens defineres og hvordan de skal måles.

I tilfeller hvor vi har betydelige mengder data vil en teknisk-naturvitenskapelig tilnærming være nyttig for å beregne risiko og sannsynlighet (Aven et al., 2004). Hampel (2006) mener også at det må finnes tilstrekkelige mengder med statistiske data for å kunne benytte denne tilnærmingen. Vi vil for eksempel kunne regne oss fram til hvor mange branner, trafikkulykker o.l. vi kan forvente oss i kommende år. Men det er viktig å bemerke seg at disse tallene ikke vil gi mening for enkeltpersoners sikkerhet, da tallene ikke gir noen informasjon om for eksempel lokasjon og tidspunkt for ulykkene.

Samfunnsvitenskapelig tilnærming til risiko

Den samfunnsvitenskapelige tilnærmingen er ikke én ting, men omhandler sosiologiske, kulturelle og psykologiske perspektiver på risiko. Det som er relevant for denne oppgaven vil, i all hovedsak, være hva den samfunnsvitenskapelige tilnærmingen generelt har bidratt med til nyere risikotilnærminger, og ikke en uttømmende forklaring av alle varianter som finnes.

Samfunnsvitenskapelig tilnærming til risiko, tar i motsetning til teknisk-naturvitenskapelig tilnærming, hensyn til menneskers risikopersepsjon. Risikopersepsjon handler om hvordan folk flest opplever, forstår og håndterer farer og risiko. Innenfor dette synet på risiko oppfattes ikke risiko som noe objektivt; risiko er sosialt konstruert og folk med ulike sosiale og kulturelle bakgrunner vil kunne oppfatte risiko forskjellig. Dette perspektivet er hensiktsmessig i undersøkelser av folks forståelse og oppfatning av risiko, da folk flest baserer sine beslutninger på langt flere faktorer enn en abstrakt sannsynlighetsberegning. Folk flest frykter en flyreise mer enn en biltur, uavhengig av ekspertens uttalelser om at sistnevnte er langt farligere. Man kan derfor si at en av styrkene til den sosiale og kulturelle tilnærmingen er at den i større grad tar høyde for kompleksiteten i vurderingen av risiko, og tar folks oppfatninger av risiko på alvor. Det tas også høyde for at mennesker med den samme kunnskapen kan bedømme risiko forskjellig (Aven et al., 2004).

Bayesiansk (kunnskapsbasert) tilnærming til risiko

Det tredje perspektivet på risiko som blir omtalt av Aven et al. (2004) er den bayesianske, også omtalt som den kunnskapsbaserte og beslutningsorienterte tilnærmingen. Dette synet skal representere en brobygger mellom den teknisk/naturvitenskapelige og den samfunnsvitenskapelige tilnærmingen. Der den førstnevnte tilnærmingen anser risiko som en ukjent objektiv og reell størrelse som kan estimeres ved hjelp av statistiske metoder, ser den bayesianske tilnærmingen på risiko som et uttrykk for usikkerhet, og ikke i seg selv en objektiv størrelse. Fullstendig kunnskap om virkeligheten finnes ikke i de fleste tilfeller, og risiko blir dermed sett på som en vurdering. Ved å følge den bayesianske tilnærmingen til risiko tildeler vi en sannsynlighet basert på usikkerhetsvurderinger, og dette inkluderer ingen referanse til en korrekt sannsynlighet. En sannsynlighet er alltid betinget den bakgrunnskunnskapen analytiker(e) besitter. Den bayesianske tilnærmingen åpner opp for både en kvantitativ og en kvalitativ forståelse av risiko. Den kvantitative kan betegnes som avgrenset, hvor det i all hovedsak fokuseres på at usikkerheten uttrykkes med sannsynligheter. Den kvalitative

forståelsen er bredere, og her kan man si at risiko er usikkerhet vedrørende utfall av en aktivitet. Det er først innenfor den kvalitative forståelse at risikopersepsjon blir relevant (Aven, 2003).

Renn (2008) mener vi er, og bør, være på vei fra tankegangen om å gjøre et skille med det realistiske og konstruktivistiske perspektivet på risiko. Han hevder at det er et lite hensiktsmessig skille, og at det fører til at perspektivene blir konkurrerende framfor å være kompatible. Renn favoriserer ingen av synene eksplisitt, men slik han framstiller en mulig løsning på håndtering av dagens komplekse trusler mener han at vi er helt avhengig av å få med både eksperter vurderinger og lekfolks oppfatninger av risiko når vi skal gjennomføre risikovurderinger. Eksperter kan tro så mye de vil at den risikoen de framstiller er en objektiv sannhet, men eksperter vil alltid møte andre eksperter som mener noe annet, og hvem er det da som sitter på sannheten? På samme måte er lekfolks oppfatning av risiko forskjellig; det dreier seg blant annet om ulike kulturer, disponering og kunnskapsgrunnlag som er med å danne enkeltpersoners oppfatning av risiko (Renn, 2008).

Trefaktortilnærmingen

Trefaktortilnærmingen er en tilnærming utformet spesifikt for beskyttelse mot tilsiktede uønskede handlinger og sikringsrisikoanalyse. Tilnærmingen inkluderer de tre parameterne verdi, trussel og sårbarhet, og ut fra disse kan man finne risikonivået (NS 5832:2012). Den vitenskapelige bakgrunnen for denne tilnærmingen er vanskeligere å få grep om enn de andre tilnærmingene som er redegjort for. Joakim Barane (2014), leder i arbeidsgruppen for NS 5830 og sekretær i arbeidsgruppen for NS 5831 og NS 5832, har i en kronikk forsøkt å redegjøre for det teoretiske fundamentet, og det velges å ta utgangspunkt i det.

Den første teorien som nevnes som relevant er *teorien om rasjonelle valg*. ”Teorien tar utgangspunkt i at individene i samfunnet er rasjonelle aktører, og at ligger en bevisst mål-middel-kalkyle til grunn for deres handlinger”. Dette mener Barane (2014) er med på å redegjøre for den grunnleggende forskjellen mellom sikringsrisiko og risiko relatert til safety-hendelser. Han identifiserer også dette som grunnlaget for det meste av academia innen sikring.

Videre gjøres det rede for *rutineaktivitetsteorien*, som forutsetter at tre faktorer må være tilstede for at en uønsket handling kan skje: mål, motivert gjerningsperson og fravær av en kvalifisert beskytter. Her vil endring i én av faktorene føre til at forutsetningene endres for en uønsket hendelse, som Barane hevder er selve essensen i sikringsfaget.

Til slutt legges ATP-teorien til som teoretisk fundament. Dette er en teori utviklet av Giovanni Manunta (1999) hvor sikring defineres som $(S = f(A, P, T))$ S i): *en funksjon mellom beskytteren (P) som opptrer som motsatsen til en trusselaktør (T) for å beskytte en verdi (A)*. Dette foregår innenfor en bestemt situasjon (S). Denne teorien identifiseres av Barane (2014) som hovedteorien bak trefaktortilnærmingen til risiko innenfor security.

3.3 Risikoanalyse

Risikovurdering, risikoanalyse og risikostyring brukes i dagligtalen om hverandre, men for akademiske formål er det viktig å gjøre et skille mellom disse elementene for en bedre oversikt og forståelse. Aven (2010) og Rausand og Utne (2009) forklarer at risikoanalyse sammen med risikoevaluering er risikovurdering, og sammen med risikokontroll/håndtering har man risikostyring (se figur 1.1).

Kort sagt omhandler risikoanalyse identifisering av initierende hendelser og analyse av tilhørende årsaker og konsekvenser. Rausand og Utne (2009:3-4) skriver at risikoanalyse kan gjennomføres ved å besvare tre spørsmål: i) hva kan gå galt?, ii) hva er sannsynligheten for at de uønskede hendelsene inntreffer? og iii) hvilke konsekvenser kan hver av de uønskede hendelsene medføre? I analysen beskrives risikoene og usikkerhetene uttrykkes, og gjennom dette skal det gi en bedre innsikt om risiko i forbindelse med en aktivitet, system eller et objekt (Aven, 2007).

3.3.1 Sikringsrisikovurdering

Sikringsrisikovurdering referer til verdivurdering, trusselvurdering, sårbarhetsvurdering, valg av scenarioer og presentasjon av risikobildet. Sammen med vurdering av strategi og vurdering av tiltak defineres dette som sikringsrisikoanalyse i NS 5832 (2014:3). Det er viktig å presisere at NS 583x-serier har snudd om på betydningen av vurdering og analyse fra NS 5814. I denne oppgaven velges verdi-, trussel-, og sårbarhetsvurdering, altså sikringsrisikovurdering, opp mot det som ovenfor (kap 3.3) ble definert som risikoanalyse.

Verdivurderingen har som formål å kartlegge virksomhetens verdier, og vurdere hvilke av disse som er viktigst for virksomhetens oppdrag og leveranser. Dette fordrer at man på en systematisk måte vurderer hvilke konsekvenser det kan få dersom verdiene skulle rammes (NSM, 2016:11).

Trusselvurdering innebærer en beskrivelse av det gjeldende trusselbildet som ønskes beskyttet, hvor fokuset skal være på reelle og potensielle trusselaktørers intensjon om og kapasitet til å ramme virksomheten (NSM, 2016:14).

På bakgrunn av verdi- og trusselvurderingen anbefales identifisering og valg av scenarioer. Hensikten med dette er å få fram sårbarhetene som er relevante for analysen. Her gjennomføres en *sårbarhetsvurdering* som skal vise eventuelle gap mellom innførte tiltak og en trusselaktørs intensjon og kapasitet (NSM, 2016:19).

Til sist gjøres en sammenstilling av faktorene basert på de tre foregående vurderingene, hvor formålet er å beskrive hver enkelt risiko som virksomheten er eksponert for. I denne samlede vurderingen inngår også klassifisering av de ulike risikoene, og anbefalinger om å beskrive usikkerheten for hver enkelt risiko (NSM, 2016:22).

3.3.2 Ekspertvurderinger og involvering av interessenter

Et mål for risikovurderinger er å skape et grunnlag for å kunne ta de riktige beslutningene angående hensiktsmessig implementering av tiltak. Dermed er man avhengig av at kunnskapen vurderingene er basert på er så fullstendig som mulig. Et virkemiddel for å øke styrken på kunnskapen og få et bedre og mer helhetlig situasjonsbilde/forståelse av fenomenet er bruk av ekspertvurderinger. Aven et al. (2004) hevder at ekspertene som skal bidra ikke bare må kunne noe om hvordan systemet fungerer, men også vite noe om hva som kan skje for at det ikke lengre skal fungere i tillegg til å ha en formening om i hvilken grad dette kan inntreffe.

Dreyfus og Dreyfus (2005) har utviklet karakteristikk som viser utviklingen fra novise til ekspert. Dette kan være karakteristikk som kan være nyttig å vurdere når interessenter skal involveres.

Tabell 3.1 *Karakteristikk av interessenter*

Novise	Får kunnskap ved å delta i situasjoner, og lærer etter hvert å sette kunnskapen inn i kontekst.
Kompetent person	Analytisk og faktabasert tilnærming til problemstillinger.
Profesjonell person	Kan skille ut relevante fakta i tillegg til å inneha en intuitiv problemforståelse. Løser problemer på en analytisk måte.
Ekspert	Intuitiv tilnærming til problemet og løsningen.

For terrorisierisiko er det ofte kunnskapsgrunnlaget det er knyttet størst usikkerhet til. Denne usikkerheten bør formidles, og dette kan gjøres ved å gi en vurdering av kunnskapsgrunnlaget for analysen. Flage og Aven (2009:14) foreslår fire indikatorer for å vurdere styrken og usikkerheten i kunnskapsgrunnlaget:

1. Forståelsen av fenomenet som undersøkes er forstått; modeller er fraværende eller antatt å gi dårlige resultater.
2. Antakelsene som er gjort representerer sterke forenklinger.
3. Tilgangen på relevante data og erfaringer.
4. Enighet blant ekspertene som deltar i analysen?

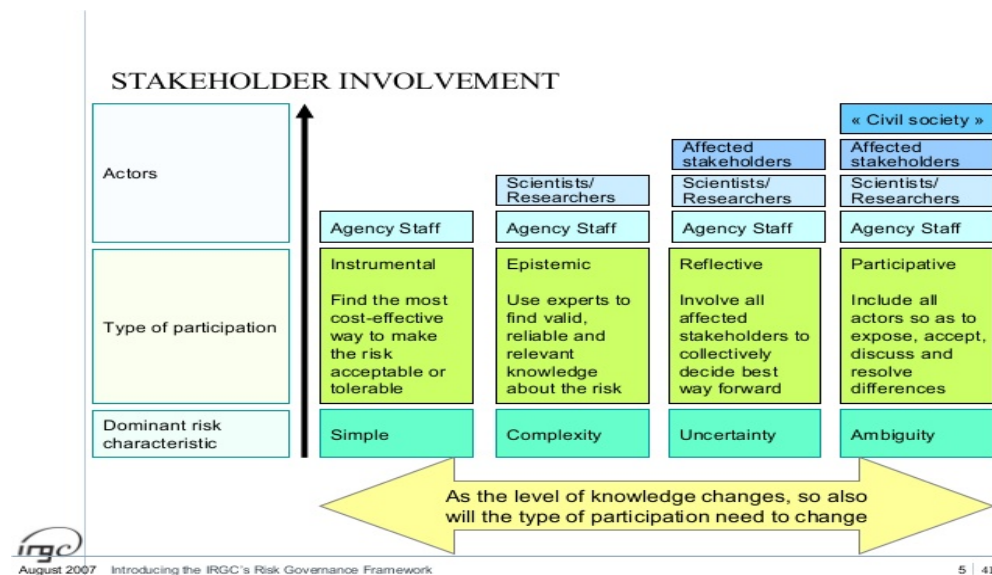
Risikostyringsprosessen innebærer beslutningstaking som vil angå flere aktører og grupper i samfunnet. På samme måte som at det er forskjellige oppfatninger mellom de som produserer risikoen og de som er eksponert for risikoen, må det også antas at det finnes ulike oppfatninger hos de som er kjent med risikoen og de som ikke er det. Ulik forståelse og oppfatning av risiko kan da også forventes å skape konflikter mellom de ulike partene (Aven og Renn, 2010). Når det gjelder involvering av eksperter og lekfolk i risikostyringsprosessen er det å forvente at de ulike deltakerne har forskjellig kunnskap og persepsjon om risikoene, og målet bør være å få med alle betraktninger og oppfatninger underveis i prosessen.

Renn (2008) mener behovet for inkludering av eksperter, interessenter og representanter bør avgjøres på bakgrunn av hvilken type risiko som skal vurderes. Han skiller mellom enkle, komplekse, usikre og tvetydige risikoer, hvor de i stigende grad har behov for bredere input fra relevante aktører.

Med *kompleksitet* menes utfordringer tilknyttet å finne forholdet mellom årsak og utfall. En kompleks risiko skiller seg dermed fra en *enkel* risiko ved at det ikke nødvendigvis finnes en åpenbar forbindelse mellom en hendelse og de konsekvenser den kan få (Renn, 2008). Dette kan skyldes flere ting. Blant annet kan det være vanskelig å få oversikt om det er flere faktorer som virker sammen eller at hendelsen får store konsekvenser i ettertid.

Usikkerhet referer til vanskeligheten med å forutsi en hendelse og dens tilhørende konsekvenser (Renn, 2008). Videre henviser han til at dette kan skyldes svakt eller manglende datagrunnlag, upassende analysemetoder og uenighet blant ekspertene. Usikkerheten kan også komme av kompleksitet i årsaks- og konsekvenskjeden.

Renn (2008) skriver at høy kompleksitet og usikkerhet kan føre til *tvetydighet*, som identifiseres som den siste risikokarakteristikken. Tvetydighet kan gi opphav til flere meningsfulle og legitime tolkninger av aksepterte risikovurderingsresultater. Det skiller mellom fortolkende og normativ tvetydighet. Den fortolkende tvetydigheten viser til uenighet om betydningen av resultatet, mens dens normative innebærer hvorvidt man enes om risikoen er akseptabel eller ikke (Renn, 2008).



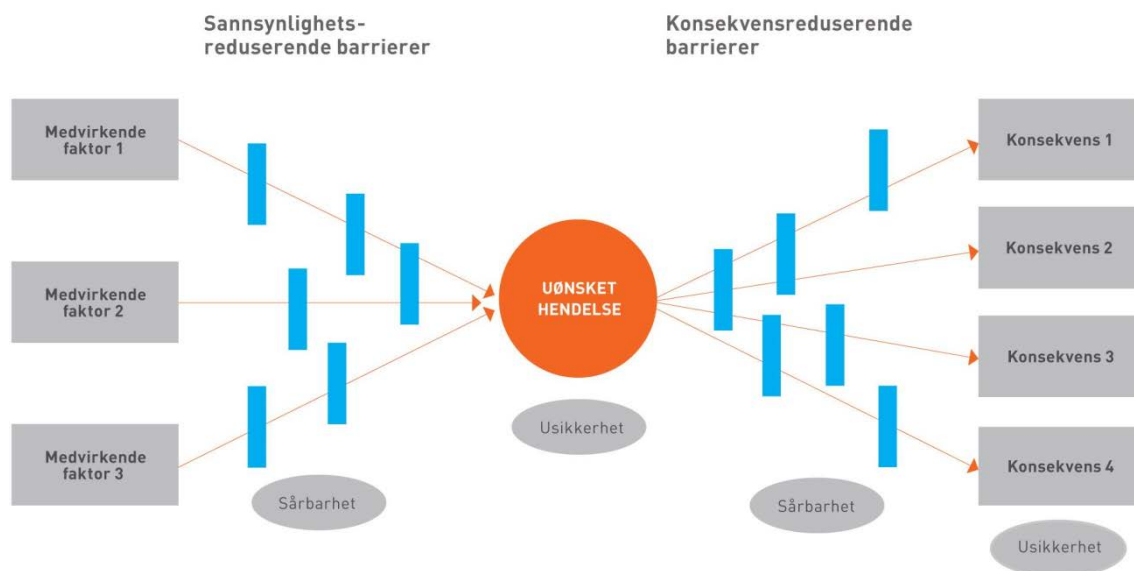
Figur 3.3 The risk management escalator and stakeholder involvement (Renn, 2008:280).

3.3.3 Ulike metoder for risikoanalyse

3.3.3.1 Bow-tie diagram

Bow-tie-diagram kan brukes for å beskrive og visualisere risikoene i en risikoanalyse. Diagrammet gjennomføres for hver enkelt risiko man vurderer som relevant for sin virksomhet, hvor årsakene og konsekvensene beskrives på hver sin side. Det vil med diagrammet være mulig å uttrykke hvilke barrierer som finnes, både årsaks- og konsekvensreducerende (Rausand og Utne, 2009). Ved å benytte bow-tie-diagrammet får man en oversikt over hvilke hendelser som kan inntreffe, årsaker og konsekvenser, men siden man tar for seg hendelse for hendelse viser den ikke noen oversikt eller sammenligning over alle risikoene. Diagrammet kan likevel sies å gi et godt grunnlag for å plassere de relevante risikoene i en risikomatrix.

«Bow tie»-modell for risikoanalyse

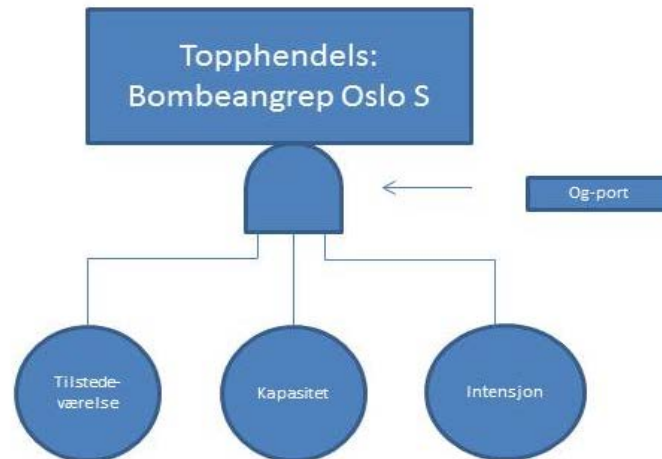


Figur 3.4 Bow tie- modell for risikoanalyse med usikkerhet (DSB, 2014:27).

3.3.3.2 Feiltreanalyse

I en feiltreanalyse er utgangspunktet den initierende hendelsen og tar for seg årsakene til at en hendelse inntreffer (Aven, Røed og Wiencke, 2008). Feiltreanalyse kan både gjennomføres kvantitativ med tallfestede sannsynligheter, og kvalitativt for å få en oversikt over årsakssammenhengene. Fordelen med å tallfeste sannsynlighetene er at man kan regne ut sannsynligheten for at en hendelse skal inntreffe. Fordelen med å framstille det kvalitativt, særlig for en potensiell terrorhendelse, er at det kan vise de ulike elementene som må være tilstede for at hendelsen kan inntreffe. Feiltreet vil ikke eksplisitt uttrykke usikkerheten, men vil vise at det er flere faktorer som må være tilstede for at trusselen skal være reell. For terrorhendelser kan det da forklare til mottakerne at tilstedeværelse av en potensiell

trusselaktøre ikke nødvendigvis betyr en forhøyet risiko om man samtidig vurderer at denne aktøren ikke har kapasitet til å gjennomføre et angrep.



Figur 3.5 Eksempel på et enkelt kvalitativt feiltre.

3.3.3.3 Hendelsestre

Hendelsestreanalyse benyttes for å synliggjøre ulike mulige hendelsesforløp den initierende hendelsen kan lede til (Aven, Røed og Wiencke, 2008). Denne metoden kan også gjennomføres kvantitativt og kvalitativt. Forskjellen vil være at den kvantitative vil gi sannsynlighetsberegninger og beregninger knyttet til konsekvensene. Den kvalitative tilnærmingen vil først og fremst gi en oversikt over de mulige hendelsesforløpene. En vanlig måte å gjennomføre hendelsestreanalyse på er å stille en rekke spørsmål hvor svaret er ja eller nei. For terrorhendelser vil dette være en nyttig metode for å analysere og visualisere konsekvensene en hendelse kan ha. Når analysen gjennomføres med en kvalitativ tilnærming vil det trolig også være mulig å inkludere konsekvenser som går utover tap av menneskeliv og materielle verdier. Analysen gjør det også mulig å visualisere hvordan implementerte tiltak vil påvirke konsekvensene.

3.4 Risikokommunikasjon

Kommunikasjon har ikke én allmenn akseptert definisjon, men det man kan enes om er at det handler om overføring av informasjon, og at vellykket kommunikasjon kan best oppnås når sender og mottaker har samme forståelse for ord og symboler samt felles moralsk forståelse, erfaringer og verdier (Hampel, 2006). For denne oppgaven er det ikke behov for en mer finurlig definisjon enn dette, men det er et behov for å skille mellom enveis- og toveiskommunikasjon. Enveiskommunikasjon er når budskapet formidles fra sender til mottaker uten at mottaker har

mulighet til å svare (Kaufmann og Kaufmann, 2003). Typiske eksempler på dette er informasjon vi får fra media som radio, tv og aviser. Denne kommunikasjonsformen kan egne seg når en ønsker å få ut et tydelig budskap til mange mennesker. For at budskapet skal nå fram og bli forstått krever det at budskapet er tydelig og tilpasset mottakeren. Toveiskommunikasjon åpner for at mottakeren får mulighet til å respondere på budskapet (Kaufmann og Kaufmann, 2003).

For å tydeliggjøre hva som vil være fokuset i denne oppgaven anses det også som hensiktsmessig å skille risikokommunikasjon fra krisekommunikasjon. Hvor risikokommunikasjon omhandler noe som kan hende, innebærer krisekommunikasjon informasjonsutveksling om noe som har hendt (Simonsen, 2009). Den sistnevnte vil falle utenfor rammene til denne studien. Kommunikasjon identifiseres som et viktig element innenfor de fleste risiko- og sikkerhetsstyringsprosesser (Aven og Renn, 2010; Aven et al., 2004 og Jore og Njå, 2012), og da gjerne innenfor alle fasene. Simonsen (2009) erkjenner at risikokommunikasjon er krevende: *“Informasjon skal være sann og saklig. Samtidig skal den vekke folks aktsomhet og noen ganger få den til å gjøre noe eller la være å gjøre noe, men uten å skremme opp folk unødige”*. Anbefalingen hans er at det bør legges opp til en “føre-var-tilnærming” i risikokommunikasjonen inntil det er gjennomført risikovurderinger, og at de konkrete rådene om ønsket handling bør komme når vurderingene er gjort (Simonsen, 2009).

Kommunikasjon identifiseres som et viktig element innenfor alle fasene i Renns (2008) rammeverk for Risk Governance. Aven og Renn (2010:159) referer til US National Research Councils definisjon av risikokommunikasjon:

En interaktiv prosess med informasjon og oppfatning blant enkeltpersoner, grupper og institusjoner. Dette innebærer flere meldinger som omhandler selve risikoen, men også andre meldinger, som strengt tatt ikke er om risiko, men som uttrykker bekymringer, meninger eller reaksjoner tilknyttet risikomeldinger eller til juridiske og institusjonelle ordninger for risikostyring (egen oversettelse).

Videre hevder de at hovedmålet er å bidra til at interessenter og befolkningen kan ta informerte risikobaserte beslutninger. Målet med risikokommunikasjon bør imidlertid ikke være å overbevise mennesker om at analytikeren sitter med det eneste riktige svaret., men at det skal være et bidrag til å øke forståelsen slik at de selv kan vurdere hvordan de skal innrette seg etter risikoen i kombinasjon med egen kunnskap og preferanser (Aven og Renn, 2010). Fischhoff (2002) framhever behovet for å undersøke hva som er allmen kunnskap blant befolkningen, slik at man verken kommuniserer for mye eller for lite.

Organisation for Economic Co-operation and Development (OECD, 2002:52-53) gir en innføring i hvordan man kan kommunisere risikoer som er komplekse, usikre og tvetydige. Anbefalingene de gir kan ses i sammenheng med Renns (2008) rulletrappmodell (se figur 3.3). Kompleksitet fordrer til diskusjon blant eksperter; jo mer kompleks jo bredere og mer flerfaglig gruppe, hvor målet er å skape en så god beskrivelse og forklaring av fenomenet som mulig. Usikkerhet krever involvering av interessenter og utvalgte grupper av befolkningen, hvor målet er å finne balansen mellom for lite og for mye beskyttelse. Tvetydighet krever noe de kaller for

“deltakende diskurs”, hvor fokuset bør være å løse tvetydigheten og forskjellige oppfatninger om verdiene. OECD (2002) anbefaler at alle disse forskjellige diskursene kombineres eller integreres for kontroversielle risikoer.

Ulike formål med risikokommunikasjon kan, i følge Aven og Renn (2010:168), deles inn i fire kategorier:

1. *Utdanning og opplysning*: Informere om risiko, resultater av risikoanalyser og styring av risiko.
2. *Risikoopplæring og insentiver til endring i atferd*: Informere om hvordan mennesker kan håndtere risikoer de blir eksponert for.
3. *Fremme tillit til de som er ansvarlige for risikoanalyse og risikostyring*: Forsikre tilhørerne om at de som er ansvarlige for disse oppgavene handler på en effektiv, rettferdig og akseptabel måte.
4. *Involvering i risikorelaterte beslutninger og konflikthåndtering*: Gi de berørte interessenter og representanter fra befolkningen mulighet til å delta i beslutninger om risiko.

3.4.1 Kommunisere terrorisierisikoen

Tilsynelatende eksisterer det ikke noe spesifikt rammeverk for kommunikasjon av terrorisierisiko. Imidlertid er det tydelig at det er enighet, både blant akademikere og relevante ansvarlige aktører, at det er knyttet stor usikkerhet til denne risikoen, som det er avgjørende at blir formidlet (Aven, 2015; Fischhoff, 2002; Renn, 2008; Jore og Njå, 2012; Weiss, 2007; DSB, 2014 og NSM, 2016). Ansvar for å sikre mot terrorangrep er ikke lengre bare et ansvar som ligger hos offentlige myndigheter, men også hos private og offentlige virksomheter. Dette gjør at kommunikasjon om terrorisierisikoen ikke lengre bare foregår mellom eksperter. Dermed er det også behov for å gjøre informasjonen tilgjengelig for blant andre sikkerhetsledere, som ikke nødvendigvis har bred akademisk bakgrunn fra risiko- eller sikkerhetsfaget. Potensielle terrorangrep vil også ramme befolkningen, og relevant informasjon bør derfor også tilpasses dem.

Aven (2015) viser til en tendens hvor analytikere har forestillinger om at resultatene fra risikoanalyser må framstilles enkelt for at beslutningstakere skal forstå det. Videre hevder han at disse forestillingene baserer seg på myten om at beslutningstakere ikke kan forholde seg til usikkerhet. Aven (2015) mener dette er en myte og henviser til at ledere forholder seg til usikkerhet hver dag, og at det til og med er det som er en av deres hovedoppgaver.

3.4.2 Risiko med høy usikkerhet

Aven (2014) hevder at det for risikoen for terrorhendelser er behov for en mer dynamisk risikobeskrivelse enn for utilsiktede hendelser. Han begrunner dette med at hendelser på andre siden av jorda raskt kan endre risikovurderinger for terrorhendelser her hjemme, så vel som kunnskapen sannsynlighetene er basert på. For terroriserisikoen bør usikkerhet knyttes til intensjon, hensikt, mål og omfang.

Begrepet usikkerhet blir brukt på mange ulike måter. Noen hevder at risiko er et uttrykk for vår usikkerhet om framtida og at risiko derfor *er* usikkerhet. På den andre siden mener andre at begrepene risiko og usikkerhet ikke nødvendigvis har så mye med hverandre å gjøre (Rausand og Utne, 2009). Vi kan videre skille mellom *aleatorisk* og *epistemisk* usikkerhet. Den førstnevnte refererer til usikkerhet som skyldes naturlig variasjon eller tilfeldighet, og blir også kalt tilfeldig usikkerhet, iboende usikkerhet og ikke-reduserbar usikkerhet. Epistemisk usikkerhet skyldes mangel på kunnskap, og kan derfor reduseres dersom man får mer kunnskap. Uvitenheten som fører til usikkerhet kan både være bevisst og ubevisst, hvor den bevisste kan håndteres ved at dette uttrykkes i risikoanalysen. Den ubevisste er den farlige; hvor man tror man vet noe, men i realiteten er uvitende (Rausand og Utne, 2009:248-249).

Aleatorisk usikkerhet uttrykt med frekvensbasert sannsynlighet

Aleatorisk usikkerhet er som beskrevet ovenfor en tilfeldig usikkerhet. Aven og Renn (2010) beskriver dette som en frekvenstolket sannsynlighet. Her uttrykker man gjerne brøkdelen av ganger en hendelse vil inntreffe når en vurderer en uendelig populasjon av lignende situasjoner eller scenarier.

Epistemisk usikkerhet uttrykt med kunnskapsbasert sannsynlighet

Epistemisk usikkerhet uttrykker analytikerens vurderinger om verdiene til de parameterne som er benyttet (Aven, 2014:53). For terror vil trolig parameterne tilstedeværelse, kapasitet, intensjon, historikk og målvalg være relevante. Om dette ses i sammenheng med den bayesianske analysen er ideen at det først etableres sannsynlighetsmodeller som presenterer variasjonen av fenomenet (aleatorisk usikkerhet). For terror vil dette være nærliggende eksempler her hjemme og i nærområder samt en utviklingsoversikt over potensielle angripere, metoder og grupper. Deretter brukes de subjektive sannsynlighetene til å uttrykke den epistemiske usikkerheten, som ufullstendig kunnskap eller manglende kunnskap, om verdiene tilknyttet til parameterne av modellen.

Epistemisk usikkerhet skyldes mangel på kunnskap (Rausand og Utne, 2009 og Aven og Renn, 2010). Trusselbildet er i stadig endring, og terroriserisikoen skiller seg særlig ut ved at det er knyttet usikkerhet til både mulige aktører, intensjon, kapasitet, mål og tidspunkt. Den epistemiske usikkerheten uttrykkes ofte med såkalte subjektive eller kunnskapsbaserte sannsynligheter. Den betegnes som subjektiv fordi det er *noens* vurdering på bakgrunn av den kunnskap de besitter på gitt tidspunkt. Dette kan føre til at ulike analytikere får forskjellige resultater, og det blir derfor viktig å uttrykke hva som ligger til grunn for vurderingene. Aven og Krohn (2013) hevder at styrken på kunnskapen som er lagt til grunn for sannsynlighetstallene er vel så viktig som resultatene. Dersom fokuset er på å beskrive kun tallene vil det kunne skape

misforståelser og feilslutninger hos beslutningstakerne. Når en snakker om sannsynlighet er det ofte knyttet til kvantitative tall, og kritikken av subjektive sannsynligheter går blant annet på at det ikke lar seg gjøre å kvantifisere subjektive meninger, og at det dermed blir vanskelig å rangere og tallfeste risikoene.

Det vitenskapelige med subjektive sannsynligheter ligger, i følge Aven (2007), i at det er en systematisering av kunnskap som finnes om det undersøkte fenomenet, samt usikkerheten som er knyttet til konsekvensene. Sannsynlighet uttrykt på denne måten kan ses i sammenheng med den bayesianske tilnærmingen til risiko (se kapittel 3.2).

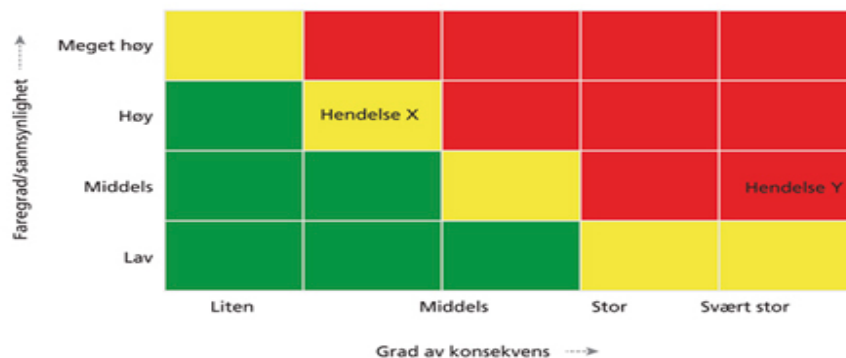
3.4.3 Framstillingsverktøy for risiko

Ved risikoanalyse, og risikostyring generelt, må man anta at det primære målet er å håndtere risiko på en tilfredsstillende måte. Ofte er det mange ulike typer risikoer som vil være relevant for analyseobjektet, og det er hensiktsmessig med verktøy som kan visualisere hvilke risikoer som er undersøkt. Herunder vil ulike framstillingsverktøy for risiko beskrives og det vil redegjøres for hvorvidt disse verktøyene gir informasjon om selve risikoen og de tilhørende usikkerhetene. Utvalget av framstillingsverktøy er basert på hva som anbefales i NS 5814 og NS 583X-serien.

3.4.3.1 Risikomatrise

En risikomatrise er et relativt enkelt verktøy for å framstille kombinasjonen av to dimensjoner av risiko: sannsynlighet og konsekvens. Som oftest brukes farger for å indikere hvorvidt en risiko er akseptabel eller ikke. Fordelen med en risikomatrise er at den gir en enkel framstilling av relevante risikoer. Utfordringene er knyttet til hva man legger i matrisen. Et problem med risikomatrisen er at den forveksles med risikoanalysen, og/eller tillegges for mye oppmerksomhet i hvordan risikoer rangeres. Risikomatrisen tar kun for seg to av dimensjonene av risiko, og tar ikke høyde for kunnskapen som ligger til grunn for resultatet (Aven, 2016). Dette kan medføre at to hendelser kan ha samme plassering i risikomatrisen, men at bakgrunnskunnskapen som ligger til grunn har forskjellig styrke uten at dette framkommer i matrisen; usikkerheten blir altså ikke uttrykt. En annen utfordring er at man kan forstå resultatet av risikomatrisen som statisk, og at endringer i forutsetningene ikke har betydning for hvor risikoen plasseres. Aven (2016) mener også at fargekodene i risikomatrisen kan være uheldig *da slike mekaniske konklusjoner om risiko i forhold til sannsynlighet og konsekvens vil være preget av vilkårlighet og ikke fange opp viktige sider ved beslutningsproblemet.*

Risikomatrixe



Figur 3.6 Eksempel på en tradisjonell risikomatrixe

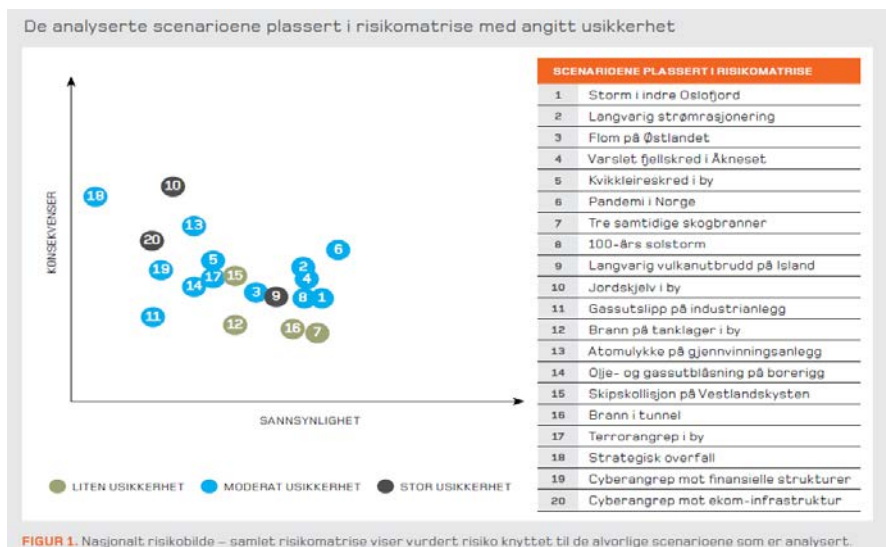
Selv om risikomatrixe tradisjonelt er en framstilling av risiko som kun tar for seg sannsynlighet og konsekvens, betyr ikke det at det er den eneste måten en kan benytte risikomatrixe. Aven, Røed og Wiencke (2008) mener for eksempel at man kan merke konsekvenskategorier med farget tekst for å synliggjøre usikkerheten i matrixe. DSB (2013 og 2014) viser også alternative framstillinger av risikomatrixe i NRB for 2013 (figur 3.7) og 2014 (figur 3.8).

Scenariorene plassert i risikomatrixe



FIGUR 25. Nasjonalt risikobilde - samlet risikomatrixe viser vurdert risiko knyttet til de konkrete verstefallsscenarioene som er

Figur 3.7 Risikomatrixe fra NRB 2013 med sannsynlighet og konsekvens (DSB, 2013:12).



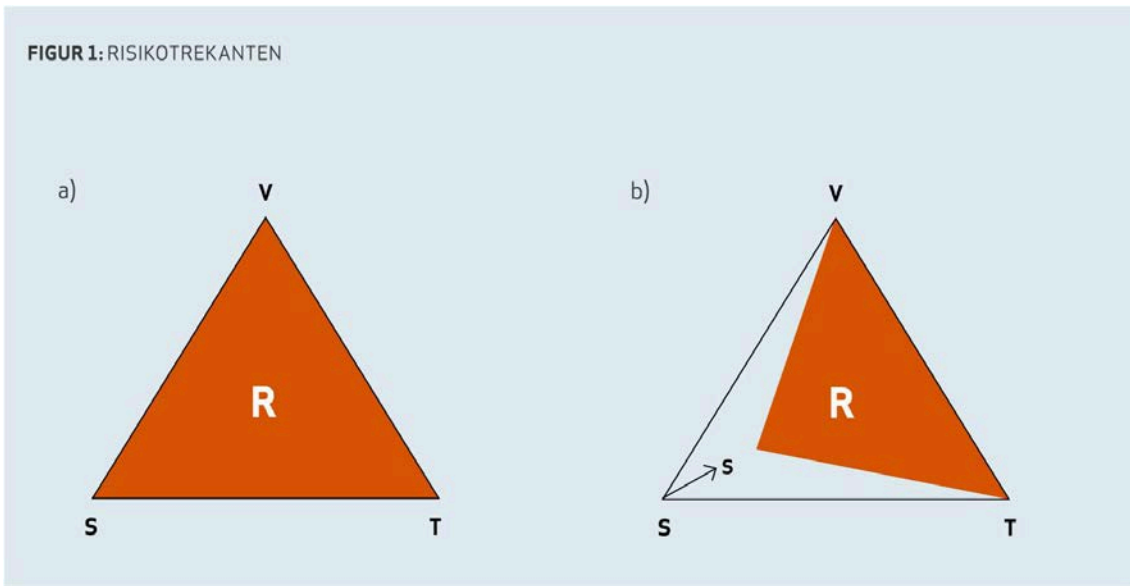
Figur 3.8 Risikomatrikse fra NRB 2014 med sannsynlighet, konsekvens og usikkerhet (DSB, 2014:9).

Figur 3.7 og 3.8 viser to ting som er relevant for denne oppgaven. For det første har DSB (2014) ved hjelp av ulike farger uttrykt hvilke av scenarioene som er mer eller mindre usikre. For det andre har de i NRB for 2014 lagt til tilsiktede handlinger i risikomatriksen.

3.4.3.2 Trefaktormodellen og risikotrekanten

Risikotrekanten beskriver verken sannsynlighet eller usikkerhet, og det er uklart hva som egentlig formidles bortsett fra at vurderingen er basert på faktorene verdi, sårbarhet og trussel. Trekanten til venstre i figuren under skal illustrere den totale risikoen, og den til høyre skal vise risikoen etter implementerte tiltak (NSM, POD og PST, 2015). Risikotrekanten gir, i motsetning til risikomatriksen, ingen oversikt over hvilke andre trusler eller risikoer som eventuelt er vurdert. Dette gjør at man ikke får en oversikt over alle risikoene, samt at det ikke vil være mulig å se risikoene i forhold til hverandre og derifra gjøre prioriteringer i forbindelse med aksept. I så måte er det vanskelig å sammenligne risikotrekanten med risikomatriksen. Det vil kanskje være mer nærliggende å sammenligne den med et bow-tie diagram eller andre analyseverktøy, som feiltre og hendelsestre, som på samme måte tar for seg hendelse for hendelse.

FIGUR 1: RISIKOTREKANTEN



Figur 3.9 Risikotrekanten (NSM, POD og PST, 2015:19).

4 Metode

Vitenskapelige metoder angir hvordan man skal framskaffe kunnskap og utvikle teorier i et bestemt fagområde, og hvordan man skal sikre at kunnskapen og teoriene oppfyller kravene til vitenskapelig kvalitet og relevans på det aktuelle fagområdet (Grønmo, 2004:38). Dette kapitlet presenterer metoden som ligger til grunn for å besvare problemstillingen i denne oppgaven.

4.1 Undersøkellesdesign

Jacobsen (2005) skiller mellom intensive og ekstensive undersøkelsesdesign. Forskjellen er at intensive design søker å gå i dybden, mens ekstensive søker en breddekunnskap. For denne oppgaven er breddekunnskapen med et stort antall undersøkelsesobjekter mindre viktig, og valget falt dermed på et intensivt design. Fordelen med et intensivt design er at det ga mulighet til å få fram så mange nyanser og detaljer som mulig i de undersøkte fenomenene (Jacobsen, 2005). Fenomenene som undersøkes avgrenses til risikoforståelse og risikokommunikasjon i en terrorismekontekst.

4.2 Metodisk tilnærming

I denne rapporten er det valgt å benytte en kvalitativ tilnærming. Forskjellene mellom kvalitativ og kvantitativ tilnærming er omdiskutert, men den avgjørende forskjellen var muligheten kvalitativ tilnærming ga til å framstille analytiske beskrivelser framfor kvantitative statistiske generaliseringer (Grønmo, 2004). Også fleksibiliteten valgt tilnærming ga ble viktig. Den kvalitative tilnærmingen gir rom for å endre undersøkelsesopplegget underveis, og dermed tilpasse opplegget om (uventede) funn skulle tilsa at dette er nødvendig (Jacobsen, 2005). Kvalitativ metode egner seg når man skal avklare nærmere hva som ligger i et begrep eller et fenomen, og når det er lite kunnskap eller informasjon om det som skal studeres (Jacobsen, 2005 og Grønmo, 2004). Kommunikasjon av usikkerhet knyttet til terrorhendelser ser ut til å være et tema som ikke er forsket mye på og en kvalitativ tilnærming anses da som den eneste riktige tilnærmingen for å besvare problemstillingen.

4.3 Forskningsstrategi

Blaikie (2009) referer til forskningsstrategi som noe som skal sørge for logikk eller et sett med prosedyrer for å besvare problemstillingen. Videre hevder han at valg av strategi er et av de viktigste valgene forskeren gjør i forbindelse med forskningsdesignet, da det er avgjørende for hvordan spørsmål som kan besvares. Innenfor samfunnsvitenskapen definerer Blaikie (2009) induktiv-, deduktiv-, retroduktiv- og abduktiv strategi som alternative måter for å oppnå den logikken som skal besvare problemstillingen.

For denne studien er det mulig å kjenne igjen elementer fra både deduktiv- og abduktiv forskningsstrategi. Problemstillingen var tidlig utformet for denne oppgaven, og deretter ble

fokuset rettet mot å innhente teori som kunne legge premissene for studien – fra teori til empiri – dette er kjennetegn på en deduktiv strategi (Blaikie, 2009 og Jacobsen, 2005). Et annet kjennetegn med deduktiv strategi er at en deduserer hypoteser ut fra teorien, og dette er ikke gjort. Det er derimot formulert noen forskningsspørsmål på bakgrunn av problemstillingen, med ønske om å fortolke observasjoner i lys av en teoretisk ramme – altså har studien også en abduktiv side.

I denne studien er det samlet inn teori om både risiko, terrorisme og kommunikasjon og deretter undersøkt i lys av empiri som setter dette i en terrorismekontekst. Dette vurderes som å være i tråd med Danermarks et al., (1997) definisjon av abduksjon. Altså vil teorien være startpunktet, ikke sluttpunktet. Abduktiv forskningsstrategi handler om å beskrive og rekontekstualisere det sosiale fenomenet ut fra en tenkt sammenheng, og også oppnå ny forståelse ved å analysere fenomenet i ny sammenheng (Danermark et al., 1997). Det teoretiske utgangspunktet benyttes i så måte som tolkningsramme når data skal samles inn og tolkes.

4.4 Datainnsamling

Blaikie (2009) skiller mellom *primær*-, *sekundær*- og *tertiærdata*. *Primærdata* er innsamlet av forskerne selv med det formålet å besvare et konkret forskningsspørsmål. *Sekundærdata* er ikke samlet inn av forskerne selv, men er det som kan kalles rådata. Dette kan for eksempel være offentlig statistikk eller datagrunnlaget fra et annet forskningsprosjekt som ikke har blitt analysert. *Tertiærdata* er data som er blitt analysert, enten av forskerne som samlet den inn eller av forskere som har benyttet sekundærdata (Blaikie, 2009). For denne oppgaven er det i all hovedsak benyttet sekundærdata og tertiærdata, og da hovedsakelig rapporter og andre utgivelser som de respektive aktørene har gitt ut samt artikler fra andre forskere. Nærmere forklaring på hvilke dokumenter som har vært brukt diskuteres i kapittel 4.4.2. og 4.4.3.

4.4.1 Samtaler med relevante aktører

I utgangspunktet baserer studien og resultatene seg på teoretisk analyse og dokumentstudier. Etter hvert i prosessen så meldte likevel behovet seg for å snakke med noen av aktørene som er aktuelle innenfor feltet som er undersøkt. Dette resulterte i en samtale med en representant fra DSB og en fra PST. Det var usikkert i hvilken grad informasjonen som ble samlet inn ville benyttes; om den skulle siteres direkte i analysen eller om den skulle brukes som informasjon til økt forståelse for feltet og et bedre utgangspunkt for å finne relevant data. Informasjonen ble i all hovedsak benyttet til det sistnevnte, men respondentene er også enkelte steder i analysen brukt som referanse for å bekrefte antakelser som er gjort underveis. Bruken av informasjonen som direkte sitering ble også naturlig begrenset ettersom kommunikasjon av risiko nå blir sett i lys av risikoforståelse, og ikke risikostyring, som først planlagt.

Samtalene ble gjennomført ansikt-til-ansikt, og varte i omtrent én time. For å sette samtalene inn i en metodisk kontekst er det mest nærliggende å omtale de som kvalitative åpne intervjuer. Slike intervjuer kjennetegnes av at det legges få begrensninger for hva respondenten kan si. Jacobsen (2005) hevder det åpne intervjuet egner seg når relativt få enheter skal undersøkes og

når man er interessert i hvordan enkelte fortolker og legger mening i spesielle fenomener. Det var viktig å fange opp eventuelle poenger som respondentene ville formidle, men også å sørge for informasjon om de temaene som studien omhandler. Med dette som utgangspunkt ble intervjuguiden utformet med det Jacobsen (2005) refererer til som middels struktureringsgrad, hvor det var forhåndsdefinerte tema, noen spørsmål, men ingen svaralternativ.

Samtalene ble tatt opp med lydopptaker, etter samtykke fra respondentene, og i etterkant transkribert i sin helhet. Dette ga mulighet til å få en bedre oversikt over informasjonsutvekslingen, samt at dataene kunne gjenbesøkes for oppklaring etter hvert i prosessen.

4.4.2 Dokumentundersøkelser

Dokumentundersøkelser er innsamling av data via studier av rapporter, tekster, statistikker og lignende, som er samlet inn av andre enn forskeren selv. Dette kan også omtales som sekundærdata (Jacobsen, 2005). Denne oppgaven baserer seg, i all hovedsak, på dokumentanalyse, og det har underveis i prosessen blitt vektlagt at dokumentene som er analysert er fra førstehåndskilder. Med dette menes informasjon som kommer fra de respektive etatene eller direktoratene som er ansvarlig. Dokumenter som har vært særlig relevante er norske standarder som omhandler risikovurderinger (NS-ISO 31000:2009, NS 5814:2008, NS 5830, 2012 og NS: 5832, 2014) samt utgivelser som de undersøkte aktørene har gitt ut som rapporter, veiledere og håndbøker. I forbindelse med kommunikasjonsdelen av oppgaven er det også benyttet dokumentanalyse. Her er det i tillegg til sekundærkilder også brukt tertiærkilder. Dette betyr at forfatterne av artiklene som har blitt brukt allerede har tolket sekundærdata. Blaikie (2009) hevder at en utfordring med bruk av tertiærdata er at jo lengre forskeren beveger seg fra originalkilden jo større er sjansen for utilsiktet eller bevisst forvrenging av dataen. Dette er tatt høyde for med å, så langt det lot seg gjøre, oppsøke kildene som er referert til i artiklene. Bruk av tertiærdata har også bidratt til at det er funnet ulike syn på problemstillinger, som igjen kan sies å ha gitt rom for et bredere diskusjonsgrunnlag. Kildekritiske vurderinger blir presentert i kapittel 4.5.2.

4.4.3 Forholdet mellom metode, empiri og teori

Det metodiske strategivalget ble begrunnet med ønsket om å starte med et teoretisk utgangspunkt. For det første forskningsspørsmålet, som omhandler risikoforståelse, var det mulig å besvare spørsmålet ved hjelp av empiri om de ulike aktørenes uttrykte risikotilnærming. Imidlertid ga forskningsspørsmål 2, og essensen i problemstillingen, utfordringer i forbindelse med innhenting av empiri. Begrunnelsen for valg av problemstilling var delkonklusjonen til Busmundrud et al. (2015), om at begge de undersøkte standardene hadde begrensninger i forbindelse med kommunikasjon av risiko og usikkerhet. Det viste seg også at de fleste teoretiske og empiriske bidragene “der ute” også hadde begrensninger når det gjaldt dette emnet. Det metodiske grepet for å kunne besvare problemstillingen var derfor å benytte risikokommunikasjon og usikkerhet som teoretisk utgangspunkt for forskningsspørsmål 2. Som empirisk grunnlag for å videre kunne drøfte dette opp mot risikoen for terrorhendelser var det

behov for også å benytte teori som empiri. Empirigrunnlaget for å besvare forskningsspørsmål 2, og i stor grad problemstillingen, ble dermed basert på teori med utgangspunkt i kjennetegnene ved terrorisme, samt elementer som ble ansett som viktig og sentrale i kommunikasjon av usikkerhet.

4.5 Styrker og svakheter med designet

4.5.1 Reliabilitet

Reliabilitet uttrykker hvorvidt en annen forsker som benytter de samme metodene kommer fram til det samme resultatet og er relatert til repliserbarhet og pålitelighet (Grønmo, 2003 og Thaagard, 2009). Dataen som er analysert i denne oppgaven er fortolket gjennom mine øyne og på bakgrunn av mine teoretiske utgangspunkt, og det vil derfor være vanskelig å gi et klart svar på om en annen forsker hadde kommet fram til samme svar. Det ble i metodekapitlet lagt vekt på å redegjøre for prosessene så nøye som mulig.

4.5.2 Validitet

Validitet sier noe om hvilken grad tolkningene av data representerer den virkeligheten som er studert (Jacobsen, 2005).

Grønmo (2004:122) viser til fire typer av kildekritiske vurderinger, som ble særlig viktig for sekundær- og tertiærdataen benyttet i denne oppgaven:

Tilgjengelighet: Dette omhandler hvorvidt det finnes tilgjengelig data for å besvare problemstillingen. Når det gjelder forskning innenfor security-feltet, og særlig for terrorisme, er mye av den relevante informasjonen sikkerhetsgradert. Dette vil si at disse dokumentene ikke har vært tilgjengelig i masterprosessen, og tilgang på disse dataene ville fortsatt vært befestet med utfordringer angående referering og gjengivelse i en åpen rapport. I følge Grønmo vil manglende tilgjengelig data potensielt sett kunne skape skjevhet i analysen, og dette har vært en reell problemstilling. I analysen er det, i all hovedsak, den teknisk/naturvitenskapelige-, bayesianske- og trefaktortilnærmingen til risiko som er vurdert i forbindelse med hvordan risiko forstås og kommuniseres. De to førstnevnte er basert på et bredt teoretisk grunnlag og er bakgrunnen for flere anerkjente risikobaserte styringsprosesser. Trefaktortilnærmingen er derimot en relativt nylig introdusert styringsprosess rettet spesifikt mot tilsiktede uønskede handlinger, hvor det naturligvis ikke eksisterer samme mengde teori og empiriske eksempler. Dette er forsøkt å ta høyde for ved å konsentrere analysen om den uttrykte risikoforståelsen hos de respektive aktørene, og hvilke føringer de ulike tilnærmingene legger for risikoanalyse. Videre er det gjort antakelser basert på teoretiske betraktninger, hvor dette også er uttrykt som antakelser, og ikke bastante fakta. I diskusjon av disse ble det også viktig å begrunne antakelsene, enten med teoretiske betraktninger og/eller empiriske funn. Manglende tilgjengelig informasjon var også utgangspunktet for problemstillingen, som omhandler kommunikasjon av usikkerhet i risikovurderinger for terrorisierisiko. I følge Busmundrud et al. (2015) er kommunikasjon av risiko, og særlig av usikkerhet i begge tilnærmingene de har vurdert (NS

5032 og NS 5814), en utfordring. Det ble i denne delen av analysen nødvendig å fokusere på hvilke teoretiske bidrag som fantes innenfor emnet, og deretter forsøke å komme med noen anbefalinger for hvordan dette kan gjøres i praksis. Det er så langt det lot seg gjøre forsøkt å se dette i sammenheng med eksisterende empiriske eksempler.

Relevans: For denne oppgaven har dataen blitt nøye gjennomgått, med utgangspunkt i et teoretisk rammeverk. På denne måten er informasjonens relevans vurdert underveis i analyseprosessen, og informasjonen som ikke er ansett som relevant er forkastet.

Autentisitet: Rapportene, standardene, veilederne og artiklene som er brukt i denne oppgaven er fra anerkjente statlige aktører og forskere, og det må derfor antas at disse er ekte. Hva som gjelder for kronikker og avisartikler må samme antas.

Troverdighet: Her må det tas høyde for at dokumenter kan inneholde feilaktig informasjon. I utgangspunktet er informasjonen som er benyttet vurdert som troverdig.

4.5.2.1 Begrepsvaliditet

Begrepsvaliditet referer til en form for definisjonsmessig validitet som viser i hvilken grad sammenhengen mellom indikatorer for ulike begreper svarer til (den kjente) sammenhengen mellom disse begrepene (Grønmo, 2003). Bare i min problemstilling er det fire begreper uten en allment akseptert betydning: kommunikasjon, usikkerhet, risiko og terrorisme. Det er derfor lagt vekt på å definere begrepene underveis, og forklare hva som menes med dem i denne oppgaven. Relevante begreper er også redegjort for innledningsvis i tabell 2.2, og ulike definisjoner i standardene er beskrevet i kapittel 2.1. En del av hensikten med denne oppgaven er å se hvordan ulike forståelser av risiko kan påvirke hvordan man definerer og kommuniserer risikoen for terrorhendelser, og derfor kan det sies at forskjellige forståelser av begreper var en del av utgangspunktet for oppgaven. For å kunne diskutere disse begrepene var det viktig å ikke på forhånd ta stilling til hva som er den "korrekte" definisjonen av for eksempel risiko, sannsynlighet og terrorisme.

5 Analyse

I dette kapitlet vil det empiriske grunnlaget for studien analyseres. Delkapittel 1 og 2 inneholder en beskrivelse av PST, NSM og DSBs risikotilnærming samt deres bruk av ekspertvurderinger og involvering av interessenter. Det blir deretter forsøkt å belyse ulike forståelser av sannsynlighet med bakgrunn i PSTs uttalelser om numerisk sannsynlighet og en påfølgende debattinnleggrunde i Dagens Næringsliv (DN). Delkapittel 4 og 5 redegjør for usikkerheten som kjennetegner risikoen for terrorhendelser. I delkapittel 5.6 blir sentrale elementer vurdert som viktig i kommunikasjon av terroriserisikoen identifisert og beskrevet.

5.1 Relevante aktørers tilnærming til risiko

I Norge er det flere etater og direktorater som arbeider med å forebygge, vurdere, håndtere og kommunisere tilsiktede uønskede handlinger. I dette delkapitlet vil det forsøkes å redegjøre for noen av de ulike aktørenes risikoforståelse. Utvalget er basert på hvem som vurderer og håndterer tilsiktede uønskede handlinger i Norge, på strategisk nivå. Det er viktig å påpeke at aktørene som er undersøkt har ulike mandater. Den som skiller seg mest ut er PST, som har fokus på trusselvurderinger framfor risikovurderinger. De har likevel redegjort for sin risikoforståelse på sine hjemmesider og har, sammen med NSM og POD, bidratt til veilederen “Terrorsikring”, og er dermed tatt med som en relevant aktør.

Politiets sikkerhetstjeneste (PST)

PST benytter ikke eksplisitt begrepet risiko i sine trusselvurderinger, men benytter trusselbegrepet. De har ingen definisjoner av begreper i sin årlige utgivelse “Trusselvurdering” og heller ingen definisjon av risiko blir gitt i deres utgivelse “Terrorsikring” (NSM, POD og PST, 2015). I utgivelsen blir det referert til at veilederen for terrorsikring baserer seg på NS 583X-serien, og det er derfor nærliggende å anta at de benytter trefaktortilnærmingen til risiko. I veilederen er det også presisert under “vurdering av ren risiko” at vurderingene ikke er kvantitative, men kvalitative, begrunnet med at det er vanskelig å anslå trusselaktørens intensjon. Ut i fra dette vil resultatene preges av en viss grad av usikkerhet (NSM, POD og PST, 2015:19). Det defineres ikke hva de legger i begrepet usikkerhet eller hvordan den skal håndteres eller kommuniseres.

Trusselbegrepet er heller ikke definert i “Trusselvurdering 2015”, og må også derfor forstås ut i fra hva de legger i begrepet i NS 583X-serien: “*Mulig uønsket handling som kan gi en negativ konsekvens for en entitets sikkerhet*” (NS 5830:2012, s. 4). Det at trusselbegrepet vektlegges framfor risikobegrepet hos PST kan ses i sammenheng med deres primære oppgave, som i all hovedsak er å forhindre at et angrep skal skje. Det er trolig også mer nærliggende å benytte trusselbegrepet framfor risikobegrepet i den åpne trusselvurderingen da den ikke retter seg mot et spesifikt system eller objekt, men er relevant for Norge som nasjon. Det er likevel formuleringer i den åpne trusselvurderingen som gjør det mulig å argumentere for at flere parametere enn trussel er vurdert. For det første er det rettet fokus mot trusler mot myndighetspersoner (PST, 2016), som kan tolkes som at de har vurdert dette som en *sårbar* og

målattraktiv gruppe. For det andre er det i løpet av utgivelsen definert noen *verdier*, som skjermingsverdig informasjon og opprettholdelse av tillit hos befolkningen. For det tredje kan det i tillegg argumenteres at det er gjort en form for sannsynlighetsvurdering; i den åpne trusselvurderingen er statlig etterretningsvirksomhet, ekstrem islamisme, høyreekstreme og venstreekstreme, og deres intensjoner og kapasiteter redegjort for (PST, 2016). Dette må være rimelig å tolke dithen at det er disse aktørene PST forventer at er sannsynlig, eller mulig, at skal angripe Norge.

Bård Olsen (2013), seksjonsleder i PST, forsøker å gi en innføring i deres risikoforståelse på PSTs hjemmesider. Her bekreftes det at trefaktortilnærmingen til risiko benyttes av PST. Det som framkommer som utfordrende er hans forståelse av sannsynlighet som en utelukkende matematisk term, hvor dette ikke kan benyttes for terrorhendelser da det finnes lite empiri å bygge på. Om dette er representativt for PSTs forståelse av risiko kan det se ut som de mener det er nødvendig med en bred samfunnsvitenskapelig og kvalitativ tilnærming til risiko, som er forenlig med en bayesiansk tilnærming. Likevel har de en for snever forståelse av bruk av sannsynlighet, som kan sies å henge fast i den naturvitenskapelige tilnærmingen til risiko.

Nasjonal sikkerhetsmyndighet (NSM)

NSM bruker samme definisjon av begrepet risiko som PST, hvor trefaktortilnærmingen anbefales for risikovurdering for sikring. I sin nylige utgitte håndbok innenfor dette emnet gir de en langt tydeligere forklaring og definering av begreper enn det som finnes hos PST. De presiserer at for risikovurderinger for tilsiktede uønskede handlinger er det mer nyttig å se på risiko som en funksjon av verdi, trussel og sårbarhet enn en funksjon av sannsynlighet og konsekvens (NSM, 2016a). I håndboken henviser de også til usikkerhet som de poengterer at alltid vil være knyttet til risikovurderinger og analyse. *“Usikkerheten ligger i informasjons- og datagrunnlaget, organiseringen, kompetanse hos deltakende, bruk av metode, vurderinger underveis i analysen, presentasjon av resultater, valg av og effekt av tiltak, med mer”* (NSM, 2016a:5).

NSM viser også til en bredere forståelse av sannsynlighet hvor de beskriver at dette ofte benyttes til å beskrive usikkerhet, og at de legger til grunn at man for tilsiktede handlinger med sannsynlighet mener “mulighet for”. De viser også til sannsynlighet basert på historikk og estimerte sannsynlighetsangivelser; basert på en blanding av faglige metoder og bedømmelse. De skriver også at usikkerhet må beskrives for faktorene som vurderes, og har både for trusselvurderingen og sårbarhetsvurderingen foreslått egne rubrikker for usikkerhet. Selv om NSM anerkjenner at sannsynlighet kan benyttes både basert på tall og empirisk data, og basert på bedømmelse av den kunnskapen analytikeren besitter virker de motvillige til å benytte det i videre anbefalinger i håndboka. På den ene siden kan dette ses på som at de tar en informert beslutning hvor de har forståelse utover en matematisk sannsynlighet. På den andre siden benytter de en klassifisering for verdi, trussel og sårbarheter fra lav, moderat, høy og svært høy. Den samme klassifiseringen benyttes for å rangere de identifiserte risikoene i forhold til hverandre (NSM, 2016a). Det kan derfor være vanskelig å forstå om de egentlig gjør en slags sannsynlighets/mulighetsvurdering, men kaller det for noe annet. Busmundrud et al. (2015: 42)

uttrykker det samme, og har identifisert at trefaktortilnærmingen har en implisitt tretrinns vurdering som innebærer sannsynlighet:

1. Det er bare trusler man har fantasi til å tenke seg som blir tatt med. Det man ikke klarer å tenke seg er **usannsynlig**. Her ligger det en første sannsynlighetsvurdering.
2. Når man ser på de forskjellige scenarioene, sammenstillingen av trussel og verdi, vil man kanskje komme fram til at noen scenarioer er lite aktuelle. Noen hendelser er rett og slett **mindre sannsynlig**, og tas ikke med videre. Her er sannsynlighetsvurdering nr. 2.
3. Når konsekvensen utredes kan man kanskje finne at verdien likevel ikke er sårbar for det scenarioet som slapp gjennom siling nr. 2. Her får man sannsynlighetsvurdering nr.3 (Busmundrud et al., 2015:42).

Direktoratet for samfunnssikkerhet og beredskap (DSB)

Innledningsvis i NRB 2014 redegjør DSB for at de, på samfunnsnivå, har gått bort fra avgrensede tekniske risikoanalyser, og har erstattet det med samfunnsvitenskapelige metoder for å fange opp et bredere spekter av konsekvenser. DSB (2014) legger en subjektivistisk tilnærming til risiko til grunn for sine vurderinger, og er tydelig på at det alltid er *noen* som vurderer risiko, og at risiko derfor aldri har en sann objektiv størrelse. Videre henvises det til flere typer usikkerhet i NRB: Epistemisk usikkerhet knyttet til kunnskapsgrunnet, metodisk usikkerhet knyttet til hvor egnet valgt metode er for å analysere de aktuelle risikoene og aleatorisk usikkerhet tilknyttet tilfeldighet (DSB, 2014:21). Sistnevnte anses som mindre relevant da risikoanalysene i NRB hovedsakelig baseres på kvalitativ kunnskap, og ikke statistikk. Det påpekes at tidligere hendelser kan være med å belyse og skape økt forståelse av fenomenet som undersøkes, men kommer til kort som eneste grunnlag for risikoanalysen. Usikkerheten for scenarioene i NRB er beskrevet gjennom kunnskapsgrunnet for analysen og resultatenes sensitivitet for endringer i forutsetningene (kapasitet og hensikt for tilsiktede hendelser) (DSB, 2014:22). DSBs tilnærming til risiko kan sies å være forenlig med Aven og Renns definisjoner og ontologiske ståsted.

I metodedokumentet for NRB "Framgangsmåte for utarbeidelse av nasjonalt risikobilde (NRB)" skriver de at de for tilsiktede handlinger tar utgangspunkt i risikodefinsjonen fra NS 5830:2012. Det framkommer ikke ut fra noen av scenarioene som omhandler tilsiktede handlinger (terrorangrep, strategisk overfall, cyberangrep og skoleskyting) hvordan de eventuelt har operasjonalisert dette. En tydelig operasjonalisering av bruken av trefaktormodellen sammen med bruk av uttrykt sannsynlighet og usikkerhet kunne kanskje forent de to tilnærmingene på en hensiktsmessig måte. Hvis det er slik at de benytter denne definisjonen bør det i så fall komme tydeligere fram i scenariobeskrivelsen og resultatet av analysen.

5.2 Risikoanalyse og involvering av interessenter

Bruk av ekspertvurderinger betraktes i denne oppgaven som et nyttig verktøy for både å kunne få en felles risikoforståelse og derav kunne kommunisere risikoen effektivt og forståelig. Ekspertvurderinger blir ikke uttrykt som et verktøy anbefalt i dokumentene som omhandler trefaktortilnærmingen, med unntak av at det i terrorveilederen blir nevnt at man ved mangel på kunnskap kan innhente ekspertise (NSM, POD og PST, 2015). Håndboken til NSM (2016) nevner ingenting om sammensetning av analysegruppen. DSB (2014) benytter ekspertvurderinger i alle sine scenarioanalyser.

For alle scenarioene som er presentert i NRB er ekspertanalyse benyttet som metode (DSB, 2014). Hvordan ekspert er definert vises ikke til, men samtalen med Midtgård viser at de søker en sammensetning i gruppen som kan gi best mulig forståelse av fenomenet som analyseres. Gruppene består av representanter fra fagansvarlige myndigheter og relevante etater, og Midtgård (2016) presiserer: *“Vi har en ganske Rennsk tankegang når det gjelder involvering av også lekfolk i vurderingene, det er ikke bare eksperter som får si noe”*. DSB har også en innretning hvor de søker å gjøre all informasjon brukt i NRB ugradert, og dermed tilgjengelig for alle (Midtgård, 2016).

Midtgård (2016) presiserer at de for NRB vurderer usikkerhet i forbindelse med kunnskapsgrunnlaget og sensitivitet. Med sensitivitet menes: *“Små endringer i forutsetningene kan få store konsekvenser for resultatene av analysen. Hvis små eller veldig marginale endringer kan bety veldig mye for resultatet er resultatene veldig sensitive, og da øker usikkerheten”* (Midtgård, 2016).

Midtgård (2016) påpeker at sårbarhetsanalysene de gjennomfører viser at utilsiktede hendelser ofte blir mer komplekse enn de tilsiktede. Dette begrunnes med at en terrorhendelse i liten grad påvirker kritiske samfunnsfunksjoner, mens et ekom-bortfall eller en naturhendelse gjør det i stor grad. Kritiske samfunnsfunksjoner ses i forbindelse med kritisk infrastruktur og defineres som: *“Kritisk infrastruktur er de anlegg og systemer som er helt nødvendig for å opprettholde samfunnets kritiske funksjoner som igjen dekker samfunnets grunnleggende behov og befolkningens trygghetsfølelse”* (NOU 2006:6, s. 32).

Vastveit, Njå, Braut og Holte (2012) diskuterer ekspertvurderinger i forbindelse med Nasjonalt risikobilde, og hevder vurderingene kan brukes til:

å tildele sannsynlighet til basishendelser, adressere og tildele sannsynlighetsfordeling til parameterne, etablere passende modeller av den ”virkelige verden”, sørge for scenariobeskrivelser og utvikle anslag og gjøre antakelser og kommunisere anbefalinger til beslutningstakere (Vastveit et al., 2012:1407).

Det som skiller tilsiktede handlinger fra utilsiktede hendelser er at sannsynlighetsvurderingen gjøres ut fra kapasitet og intensjon fra aktører, samt sårbarheten for objektet, mens fokuset på historisk data er større for utilsiktede hendelser (Vastveit et al., 2012).

Siden kunnskapen som ligger til grunn for vurdering av tilsiktede handlinger er særst viktig anses Flage og Avens (2009) indikatorer for vurdering av styrken i kunnskapsgrunnlaget (se s. 24) som relevante å ta stilling til av DSB.

5.3 Sannsynlighetsdebatten i media

I november 2014, i en strengt hemmelig orientering, informerte PST regjeringen om at det er mellom 60 og 90 % sjanse for at Norge blir utsatt for et islamistisk terrorangrep i løpet av det neste året (Hultgreen, 2014). Denne uttalelsen fraviker fra hvordan PST vanligvis uttrykker sine vurderinger, da den inkluderer tallfesting av sannsynlighet. Formuleringen av sannsynligheten står også i kontrast mot det PST, sammen med POD og NSM, anbefaler i veileder for terrrorsikring (2015). Denne veilederen baserer seg på NS 583X-serien, og her foreligger det, som nevnt, ingen retningslinjer for bruk av sannsynlighet. Tidligere benyttet PST en verbal skala for å definere trusselnivået:

Tabell 5.1 PSTs tidligere karakterisering av det nasjonale trusselnivået

LAV	Sannsynligheten for en terroraksjon er lav. En eller flere aktører kan ha intensjoner om, men trolig ikke kapasitet til, å ramme bestemte interesser.
MODERAT	Sannsynligheten for en terroraksjon er moderat. En eller flere aktører har intensjoner om og kapasitet til å ramme bestemte interesser.
HØY	Sannsynligheten for en terroraksjon er betydelig. En eller flere aktører har intensjoner om og kapasitet til å ramme bestemte interesser. Det foreligger en spesifikk trussel.
EKSTREM	Sannsynligheten for en terroraksjon er ekstremt høy. En eller flere aktører har intensjoner om å ramme bestemte interesser. Det foreligger en spesifikk trussel. Ingen ytterlige advarsler kan påregnes før en aksjon iverksettes.

I 2013 skrev også analysesjef i PST Jon Fitje Hoffmann et innlegg hvor han forsvarer at PST ikke lengre benytter sannsynlighetsskalaen. Begrunnelsene går blant annet på at sannsynligheten ikke vil være lik i hele landet. Det vil dermed ikke være hensiktsmessig, både i forbindelse med kostnader og relevans, å anbefale nasjonale tiltak når trusselen er lokal framfor nasjonal. Han påpeker også at bakgrunnsinformasjon de baserer seg på som regel ikke er verifisert og derfor er usikker. Han mener nivåene PST benyttet framstår som konkluderende, og at usikkerheten ikke kommer fram, og at jo mindre informasjon de har, jo lavere blir trusselnivået. Det at trusselnivået er bestemt mener også Hoffmann vil føre til at endringer i informasjonen ikke

framkommer, samtidig som det ville vært svært forvirrende å stadig endre trusselbildet (Hoffmann, 2013).

Uttalelsen deres om sannsynlighet for terrorangrep i Norge virker forvirrende ut fra deres tilknytning til NS 583X-serien og begrunnelsen for å slutte med sannsynlighetsskalaen. På den ene siden er nok sannsynligheten befestet med mye gradert informasjon, som vi grunnet lovmessige årsaker ikke har tilgang på. Denne informasjon gir nok også trolig en bredere forklaring på hva som ligger til grunn for tallene og hva slags implikasjoner resultatet eventuelt har. På den andre siden kan det se ut som at de har en annen holdning til sannsynlighetsbegrepet innad i organisasjonen enn utad. Om dette er tilfellet eller hva som eventuelt er årsakene til dette er ikke kjent, men det skapte en etterspørsel etter sannsynligheter, og en diskusjon i media rundt emnet i etterkant.

Flesvik (2014), daglig leder i sikkerhetsrådgivningsselskapet Aeger Group, skrev i en kronikk i Dagens næringsliv at *“PST må begynne å gi informasjon om sannsynlighet for terrorangrep, slik at andre med ansvar for risikostyring kan sette inn riktige tiltak”*. Han hevder det er problematisk at verktøyene PST benytter tilsynelatende ikke fastslår sannsynligheten for at ulike terrorangrep vil kunne inntreffe. Både for publikums forståelse for implementerte tiltak og relevante aktørers vilje til å iverksette fornuftige tiltak, mener Flesvik at det er avgjørende å begrunne dette med en viss sannsynlighet for at en terrorhendelse skal skje. Det kommer ikke tydelig fram hvilken sannsynlighet Flesvik etterlyser, men han referer til ISO 31000 som et mer hensiktsmessig rammeverk enn trefaktormodellen. Ut i fra dette er det nærliggende å anta at det ikke nødvendigvis er frekvensbaserte sannsynligheter han er ute etter, da de åpner for en kvalitativ tilnærming til sannsynlighetsvurderingen (NS-ISO 31000:2009).

Carsten Rapp (2014), tidligere avdelingsdirektør i NSM, kommer med svar til Flesvik, hvor han argumenterer for at det å fokusere på sannsynlighet for terrorangrep vil kunne gi et feil utgangspunkt for sikring mot angrep. Slik det virker i Rapps tilsvarende er han av den oppfatning av at Flesvik etterlyser en frekvensbasert sannsynlighet, da han henviser til at en tradisjonell risikometodikk ikke er tilstrekkelig for viljestyrte handlinger: *“I norsk kontekst inntreffer terrorangrep med så lav frekvens at det vil være umulig å kunne beregne sannsynligheten på en hensiktsmessig måte”*. Mærli (2014) mener også i sin kronikk at Flesvik fokuserer på feil sannsynlighet. Han hevder at sannsynligheten som etterlyses eies av angriperen og at lavfrekvente hendelser som terrorisme gjør tallfesting av angrepssannsynlighet til en hasardiøs øvelse. Framfor å fokusere på denne sannsynligheten foreslår Mærli å benytte sårbarhetssannsynligheter. Framgangsmåten her vil være å anta et angrep for å så vurdere sannsynligheten for at hendelsen kan skje gitt de eksisterende barrierene. *“Sårbarhetsvurderinger er dermed en langt mer edruelig risikotilnærming enn spekulative angrepvurderinger, hvor høyst usikker sannsynlighet presenteres med usannsynlig høy nøyaktighet”*, avslutter Mærli (2014).

Flesvik (2014b) kommer til slutt med en oppklaring hvor han henviser til at det i tillegg til analyse av empiriske data fra tidligere hendelser bør foreligge analyser av de aktører og grupperinger som kan tenkes å begå angrep mot det norske samfunn. På bakgrunn av dette vil

man, i følge Flesvik, kunne konkludere i et uttrykk for sannsynlighet. Avslutningsvis stiller han spørsmålsteget angående PSTs sannsynlighetsuttalelse: “*Har PST likevel verktøyet det trenger, men så langt unnlatt å informere offentligheten om sannsynligheten for ulike hendelser? Hva er i så fall grunnen til det?*” (ibid.).

5.4 Usikkerhet

Usikkerheten i forbindelse med terrorisierisikoen vurderes som hensiktsmessig å se opp mot PSTs indikatorer for trusselvurdering: *tilstedeværelse, kapasitet, intensjon, historikk og målvalg* (Hoffmann, 2016). Det vil trolig være usikkerhet knyttet til alle disse elementene, og det vil være behov for å innhente mer informasjon og få en forståelse av hvilken innvirkning dette har på resultatet av trusselvurderingen.

Til tross for bred enighet om at usikkerhet i aller høyeste grad er gjeldende i forbindelse med terrorisme, hevder Liu et al. (2016) at det mangler en terrorisierisikoespesifikk definisjon av usikkerhet. Slik det forstås i denne oppgaven er det den epistemiske usikkerheten, som er knyttet til bakgrunnskunnskapen, som trekkes fram som den viktigste for terrorisierisikoen (Aven, 2015; Fischhoff, 2002; Renn, 2008; Jore og Njå, 2010 og Rausand og Utne, 2009). Rausand og Utne (2009) mener epistemisk usikkerhet kan knyttes til uvitenhet, og skiller mellom bevisst og ubevisst uvitenhet. Den førstnevnte referer til det vi vet at vi ikke vet, mens den ubevisste, og den skumle, referer til noe vi tror vi vet, men som vi ikke vet. Epistemisk usikkerhet kan eksemplifiseres ved å tenke seg at man er inne lyst rom også skruer noen av lyset. I dette fremmede og mørke rommet skal man da finne ut hvilke faktiske objekter som er i rommet, og hvor de befinner seg. Sannsynligheten for hva og hvor objektene befinner seg vil ikke kunne basere seg på hyppighet og frekvens, men heller “grad av tro” (Daase og Kessler, 2007). Denne sannsynligheten utgjør dermed ikke kunnskap *om* verden, heller kan man si at den gir oss kunnskap om vår interaksjon *med* verden og inkluderer kvalitative bedømmelser angående “hva som er saken” (Daase og Kessler, 2007:428).

5.5 Kommunisere usikkerhet

Beslutningene omkring risiko angår framtiden og vil derfor være beheftet med usikkerhet både om hvordan framtiden vil bli, og hvordan vi vil evaluere ulike framtidige hendelser om de skulle inntreffe. Evnen til å tolke og kommunisere usikkerhet er derfor viktige elementer for gode beslutninger.

Som nevnt i teorikapitlet mangler det tilsynelatende et rammeverk for kommunikasjon av terrorisierisikoen. I litteratursøk i forbindelse med denne studien er det imidlertid identifisert et stort behov for økt fokus på hvordan man skal kommunisere denne risikoen, og særlig behov for å kommunisere usikkerheten tilknyttet risikoen. Liu et al. (2016) ser på kommunikasjon av usikkerhet under kriser og hevder det finnes få retningslinjer om hvordan håndtere kriser hvor det mangler kunnskap, og likeså for situasjoner preget av høy usikkerhet. De bekrefter også i innledende betraktninger at usikkerhet anerkjennes som et viktig element i risiko- og

krisekommunikasjon, men at empiriske undersøkelser og teoretiske bidrag om hvordan det skal foregå er manglende (Liu et al., 2016). Selv om artikkelen handler om kommunikasjon etter en hendelse har inntruffet vil flere av punktene som diskuteres også være gjeldende i risikokommunikasjon. Spørsmålene “*hvem/hva forårsaket krisen; antall drepte og skader på infrastruktur; hva man kan gjøre for å beskytte seg; og hvor lenge krisen vil vare*” (Liu et al., 2016:1), er definitivt spørsmål som gjør seg gjeldende, og så langt det lar seg gjøre med fordel kan besvares i risikokommunikasjon, ikke bare i krisekommunikasjon.

Liu et al., (2016) hevder at begrepet usikkerhet sjeldent er definert når det brukes i forbindelse med krisekommunikasjon. Både håndtering, kommunikasjon og forståelse av usikkerhet er temaer som har fått relativt stor oppmerksomhet innenfor psykologifeltet (Brun og Teigen, 1995; Fischhoff, 2002 og Eid og Johnsen, 2006). Også innenfor tradisjonelle risikoanalyser er usikkerhetselementet godt beskrevet, både i forbindelse med identifisering og formidling (Aven, Baraldi, Flage og Zio, 2014; Aven, 2010 og Rausand og Utne, 2008). Utfordringen med å knytte disse anbefalingene til tilsiktede handlinger, og særlig terrorhendelser er at fokuset stort sett er på kvantifisering av usikkerheten og en numerisk framstilling av denne. Det blir, særlig innenfor risikoanalysefaget, poengtert at usikkerheten tilknyttet bakgrunnskunnskapen også må uttrykkes, men ikke nødvendigvis hvordan.

5.5.1 Kommunisere usikkerhet i etterretning

For å kunne ha en mest mulig reell og oppdatert oversikt over trusselbildet er man helt avhengig av å kontinuerlig samle inn og analysere relevant informasjon. På fagspråket kalles gjerne resultatet denne prosessen gir for etterretning. Det er viktig å poengtere at etterretning ikke er sannferdig, og endringer eller tillegg i informasjonen den baserer seg på i så måte kan gjøre etterretningen man har ugyldig. For terroriserisiko er etterretning essensielt for å få en helhetlig oversikt over elementene som påvirker risikoen.

Weiss (2007) viser til at det innenfor tradisjonell vitenskap tar lang tid å skape et nytt paradigme. Det er vanlig at man jobber ut fra en hypotese, og ut fra den, over tid, forsøker å skaffe beviser slik at hypotesen kan bekreftes nok ganger til at det kan bli en sannhet. Når man jobber med slike hypoteser er en av fallgruvene at man er for selektiv i sin informasjonsinnsamling, og ubevisst søker og samler informasjon som stemmer overens med de forutbestemte hypotesene. Dette vil selvsagt være uheldig for resultatet og man vil kunne unngå informasjon som heller kunne ha ugyldiggjort de antakelser og hypotesene som var utgangspunktet.

5.5.2 Uttrykke usikkerhet med sannsynlighet

For terrorhendelser er det flere som stiller seg skeptisk til bruk av sannsynlighet. Blant annet refererer Aven (2014) til Littlewood og Strigini (2004) som hevder at security-relaterte handlinger er tilsiktet og er derfor ikke åpen for sannsynlighetsanalyser og modellering. Begrunnelsen for dette er at angriperen selv vet hva han skal gjøre, og hvor ligger da usikkerheten? For det andre mener de at sannsynligheten er vanskelig å bruke på grunn av at de

samme hendelsene ikke vil gjentas. Aven (2014) er enig i at analytikerne normalt sett ikke innehar kunnskap om når og hvordan en angriper vil angripe, og at det finnes usikkerhet. Men sannsynlighet er en måte å uttrykke usikkerhet på, og selv om den frekvensbaserte kan utelukkes på grunn av at hendelsene anses som unike, bør subjektive sannsynlighet kunne benyttes (Aven, 2014).

Mye av frustrasjonen angående bruk av sannsynlighet virker å ligge i forståelsen av selve begrepet. Noen forstår sannsynlighet som *mulighet* for at noe skal skje. Skillet mellom sannsynlighet og mulighet kan best beskrives ved å se på de engelske begrepene *probability* og *likelihood*. Probability er nærliggende å sammenligne med sannsynligheten for at noe skal skje, uttrykt med et tall mellom 0 og 1, altså en matematisk term. Likelihood kan imidlertid forstås som potensialet eller muligheten for at noe skal skje, og åpner opp for at man kan benytte både kvantitative og kvalitative metoder for å vurdere mulighetene for at en hendelse skal inntreffe (NS-ISO 31000:2009, s. 6). Allerede her kan man forstå at det blir misforståelser i forbindelse med hva som formidles, og framhever behovet for en tydeliggjøring av hva som legges i begrepene som brukes.

Aven (2010:623) mener også at sannsynlighet kan forstås på to måter:

“Sannsynlighet kan forstås som den relative hyppigheten en hendelse kan inntreffe i en hypotetisk situasjon som gjentas uendelig mange ganger”.

“Sannsynlighet er et mål for usikkerheten om framtidige hendelser og konsekvensene tilknyttet disse, sett gjennom øynene til den som vurderer, og basert på bakgrunnsinformasjon og kunnskap”.

Denne førstnevnte forståelsen kan knyttes til den naturvitenskapelige tilnærmingen til risiko og det engelske begrepet probability. Denne typen sannsynlighet er det vanskelig å se for seg at kan benyttes for terroriserisikoen. En slik sannsynlighet er i beste fall kun relevant for systemer hvor det faktisk er mulig å gjøre forsøk med lignende systemer eller bruke en form for modell som kan gi oss den informasjon vi trenger. Weiss (2007) sammenligner analyseproblematikken knyttet til usikkerhet for tilsiktede handlinger med klimaforskning. På samme måte som vi bare har en jordklode, og ingen laboratorier hvor alternative modeller av planeten kan testes med kontrollerte eksperimenter, finnes det bare ett Irak og én IS-organisasjon.

Rand Corporation (Jenkins, Willis og Han, 2016) har undersøkt hvorvidt signifikante terrorangrep øker risikoen for flere angrep. Resultatet fra undersøkelsen er basert på historiske data og statistikker over terrorangrep i USA og Europa i perioden 1970 til 2013. De besvarer spørsmålet ved å se på to ting; skjer terrorangrep i klynger og er det spesifikke datoer som er spesielt utsatt. Konklusjonen er at det mellom 1970-2002 var flere terrorangrep som skjedde i klynger, mens at angrepene mellom 2003-2013 har vært tilfeldig (se tabell 2) (Jenkins, Willis og Han, 2016:2).

Tabell 5.2 Summary of findings About Clustering of Terrorism Events

Time Period	Did Terrorist Events Occur in Non-Random Clusters?	Did clusters of Events Occur in the Wake of Larger Attacks
1970-1993	Yes	Yes, clusters appear to be related to larger events.
1994-2002	Yes	No, clusters are not explained by large events.
2003-2013	No	Clusters were not present.

Når det gjelder hvorvidt spesifikke datoer var mer typiske for terrorangrep viser undersøkelsen at datoer hvor man kanskje forventer at angrep skal skje, som 11.september, historisk sett ikke er assosiert med et større antall angrep (Jenkins, Willis og Han, 2016). Imidlertid er dagene rundt 4.juli og nyttårsaften datoer hvor det har vært et uvanlig høyt antall angrep. Dette kan trolig ses i sammenheng med at slike datoer ofte er relatert til at store folkemengder samles. På den annen side kan det for store arrangementer, som for eksempel festivaler, forventes at det er satt inn sikringstiltak, som igjen vil føre til at sannsynligheten for et angrep blir lavere, selv om den historisk sett er høy.

Den andre beskrivelsen kan knyttes til det den bayesianske tilnærmingen til risiko, hvor sannsynligheten er et subjektivt mål for usikkerhet basert på den bakgrunnskunnskapen den som vurderer besitter. I følge Aven og Renns (2010) definisjon av risiko har risikoen to hovedkomponenter: konsekvensene av aktiviteten og usikkerheten om hva disse konsekvensene vil bli. Sannsynligheter kan brukes for å uttrykke hvor stor risikoen er, og er et mål på hvor trolig det er at en hendelse skal inntreffe. Aven (2015) framhever at sannsynlighetene her kun er et redskap for å uttrykke risikoen, men at det også må tas hensyn til hva sannsynlighetene bygger på. Altså må også bakgrunnskunnskapen resultatene bygger på formidles.

5.5.3 Eksempel på kommunikasjon av terrortrusselen fra PST

24.juli 2014 informerte justisminister Anders Anundsen og PST-sjef Benedicte Bjørnland om at: “Det foreligger en konkret og tidsavgrenset terrortrussel mot Norge. ... hvem som står bak, hva målet eventuelt er og hvordan et eventuelt angrep skal gjennomføres, er ikke kjent” (Lilleåsen, 2014). Hoffmann (2016) bekrefter i samtalen med han at årsaken til at de gikk ut med denne informasjonen var at flere av deres kilder kom med etterretning som tydet på at trusselen var reell. Samtidig krevde trusselen synlige beredskapstiltak, som også skaper et informasjonsbehov hos befolkningen. Trusselvurderingen førte til økt beredskapsnivå i hele landet, hvor blant annet politiet ble bevæpnet, grensekontroller strengere og generelt økt vakthold. Situasjonen vedvarte i tre dager før beredskapen ble nedjustert 27.juli og tilbake på normalnivå 30.juli (Lilleåsen, 2014). Det ble jevnlig holdt pressekonferanser, uten at informasjonen fra myndighetene ble noe særlig mer konkret. Flere stilte seg kritisk til at PST ikke gikk ut med mer detaljerte opplysninger etter hvert som de fikk ny informasjon, og etterlyste konkrete råd om hva man som både enkeltpersoner og virksomhet skulle være oppmerksomme på, og forholde seg til.

Det var først i etterkant, når beredskapsnivået var tilbake til normalen og trusselen var svekket, vi fikk mer informasjon om trusselen. PST-sjef Bjørnland informerte på PSTs hjemmesider om at de hadde mottatt informasjon om at en gruppe personer var på vei fra Syria mot Europa, hvor hensikten skulle være å gjennomføre en terroraksjon, og Norge var et av de nevnte målene. I opplysningene PST fikk var det også informasjon om at tidsfristen var kort, og at et eventuelt angrep kunne skje i løpet av få dager (Bjørnland, 2014b). Bjørnland skriver også at offentliggjøring av trusselen kan ha forhindret trusselen, men at det er noe vi aldri får vite.

5.6 Sentrale elementer i kommunikasjon av risiko for terrorhandlinger

I dette delkapitlet vil sentrale elementer i kommunikasjon av risiko redegjøres for. Elementene som er lagt til grunn er valgt på bakgrunn av hva som er identifisert som viktige faktorer å ta hensyn til i kommunikasjon av terroriserisikoen og usikkerhet. Det er i all hovedsak dokumentstudier som har lagt grunnlaget for dette kapitlet.

5.6.1 Tillit

Det er bred enighet om at tillit er et viktig element i risikokommunikasjon (Liu et al., 2016; Rogers et al., 2007; Aven og Renn, 2010; Simonsen, 2009; Fischhoff, 2002 og Hampel, 2006). Rogers et al. (2007) hevder at risikokommunikatoren må finne den riktige balansen mellom å sørge for formidling av fakta og nyttig informasjon samtidig som de skal unngå å skape frykt. Videre skriver de at tillit er antatt å redusere usikkerhet blant befolkningen, og at det kan påvirke risikopersepsjonen og risikoaksept. Tillit kan også ses i sammenheng med usikkerhet på to måter. For det første når det gjelder mottakerens tillit til senderens aksept om at det eksisterer usikkerhet (Liu et al., 2016). For det andre vil det være relevant i forbindelse med hvorvidt kommunikatoren innrømmer usikkerheten som finnes i resultatet som presenteres (Rogers et al., 2007; Weiss, 2007 og Fishhoff, 2002).

Flage og Aven (2009) hevder at risikonivå, usikkerhetsfaktorer og risikoreduserende tiltak er viktig å formidle når risikobildet skal kommuniseres til beslutningstakere. Altså må informasjon omhandle hvorvidt risikoen er høy, lav eller typisk for systemet som undersøkes, usikkerhet knyttet til kunnskapen på gitt tidspunkt og hvilken effekt tiltak kan ha. Dette kan ses i sammenheng med Rogers et al. (2007) og Simonsens (2009) råd for risikokommunikasjon til befolkningen. Her snakker de om balansen mellom fakta og nyttig informasjon på samme tid som man unngår å skape frykt. Tillit betegnes som noe som er enkelt å miste og vanskelig å gjenvinne (Rogers et al., 2007). Det anses derfor som viktig å ta høyde for både bygging og opprettholdelse av tillit før, under og etter risikokommunikasjonsprosessen.

Rogers et al. (2007) hevder at tillit er særlig viktig når det gjelder kommunikasjon om risiko som ikke omhandler vanlige dagligdagse hendelser, og at det er særlig relevant i forbindelse med komplekse problemer, som nasjonal sikkerhet og kontraterrorisme. Kompleksiteten her referer til at mennesker trolig vil basere sin tillit på enighet og sympati heller enn nøye begrunnede argumenter. Med dette som utgangspunkt kan det trekkes direkte paralleller mellom

tillit og viktigheten ved også å inkludere hensyn til risikopersepsjon i kommunikasjon (se kap. 5.6.4).

Noe av problemet med å formidle usikkerhet til offentligheten kan, i følge Weiss (2007), ligge i analytikerens stolthet, og dens frykt for at resultatene skal underspilles. Dette kan ses på som et paradoks i forbindelse med tillit. Analytikeren er av den tro at formidling av usikkerhet kan skape mistillit til hans resultater da usikkerhet av han tolkes som noe negativt, og gjør at resultatene ikke er fullstendige. Derimot vil det fra mottakeren oppfattes som negativt og ufullstendig om ikke all informasjonen gjøres rede for, og dermed skape mistillit. Dette fordrer at analytikeren også har tillit til at mottakerne av informasjonen har kapasitet til å forstå hva som formidles, og at det ikke tas snarveier med forenkling og tilbakeholding av resultater. Utfordringen ved å kommunisere både risikoen og usikkerheten, samt eventuelle risikoreduserende tiltak relatert til terrorisme ligger i hensynet til innsynet fra potensielle trusselaktører (Rogers et al., 2007 og Daase og Kessler, 2007).

5.6.2 Ord og tallforståelse

Fischhoff (2002) mener hensyn til tall- og ordforståelse er av svært viktig betydning for hvordan risiko og usikkerhet kommuniseres. Tallforståelse refererer til forståelsen for hvor høy risikoen er. Om risiko formidles via sannsynligheter er dette tradisjonelt formidlet med et tall mellom 0 og 1, eller mellom 0-100 %, om det benyttes prosenttall (Rausand og Utne, 2009). Ordforståelse er viktig med hensyn til hva som formidles; i forbindelse med hvilke begreper som brukes og fenomenet som kommuniseres. Fischhoff (2002:6) eksemplifiserer dette med kommunikasjon av risikoen for spredning av anthrax. Her er man avhengig av at mottakerne av informasjon vet noe om anthrax, om hvem som står bak, om spredningsraten for små partikler og hvem av, for eksempel nasjonale myndigheter, som har ansvaret for håndtering.

Kommunikasjon handler om overføring av informasjon, og Hampel (2006) og Fischhoff (2002) framhever viktigheten med felles referanserammer omkring ord, symboler og verdier. Det er ikke alltid dette eksisterer, og det vil være viktig å redegjøre for hva det er som kommuniseres. For kommunikasjon av terrorismerisikoen vil det være flere definisjoner som kan komplisere informasjonsutvekslingen. Verken terrorisme eller risiko har noen entydig definisjon, og ulike definisjoner lagt til grunn vil kunne påvirke meldingen som kommuniseres.

Parameterne risikoen baserer seg på, og risikoverdien, kan også uttrykkes med ord. Eksempelvis uttrykker DSB (2014) sannsynligheten med *svært lav*, *lav*, *moderat*, *høy* og *svært høy*. Det er omdiskutert hva som oppfattes som enklest å formidle, og mest forståelig, av numeriske og verbale sannsynlighetsangivelser. Eid og Johnsen (2005) refererer til preferanseparadokset for å forklare ambivalensen i forbindelse med hvordan mennesker ønsker å gi og motta informasjon om usikkerhet: "... *de fleste foretrekker å uttrykke usikkerhet med ord (verbale sannsynlighetsbeskrivelser), mens de ønsker å motta informasjon fra andre i tall (numeriske sannsynlighetsbeskrivelser)* (Eid og Johnsen, 2005:166).

Weiss (2007) hevder at en av grunnene til at usikkerhet ikke uttrykkes ved hjelp av matematiske sannsynligheter er at mennesker har en tendens til å være ukomfortable med matematiske sannsynligheter, og har vanskeligheter med å forstå dem. Han mener at en alternativ løsning kan være å presentere en kvalitativ, muntlig skala for usikkerhet gitt at ordene som blir brukt har en klar, tydelig og forstått mening. Sjef PST Benedicte Bjørnland (2014b) hevder at bruk av sannsynlighet kan underkommunisere risikoen for terrorhendelser; deres vurderinger baserer seg på etterretning, som per definisjon er forbundet med usikkerhet, og en prosentvis framstilling av sannsynlighet vil underkommunisere en kompleks virkelighet samtidig som det øker faren for at budskapet mistolkes. Bjørnland poengterer videre at det er viktig at kommunikasjon av usikkerhet ikke forveksles med vaghet.

Fischhoff (2002) hevder det er helt nødvendig å kvantifisere estimater for risiko, inkludert de underliggende usikkerhetene, for å få til en effektiv risikoanalyse og risikokommunikasjon. Aven, Wiencke og Røed (2003) sier at man bør unngå ord som “ofte” og “sjeldent” da disse begrepene kan ha forskjellige tolkninger. De anbefaler at sannsynlighet uttrykkes som prosent, og at man hvert fall ikke kan “dekke” seg bak andre formuleringer uten å forklare hva som menes med dem (Aven, Wiencke og Røed, 2003:81). Fischhoff (2002) sier også at bruk av ord som “mulig” i sannsynlighetsangivelser framfor å benytte tall, kan skape en felle for lytterne. Begrepet “mulig” har forskjellige betydninger hos ulike personer, og ulik betydning for samme personer i forskjellige situasjoner.

5.6.3 Risikopersepsjon og atferdsteori

Begrepet persepsjon, brukt i kognitiv psykologi, refererer til den mentale prosessen hvor mennesker tar inn, håndterer og vurderer informasjon fra omgivelsene via sine sanser (Eid og Johnsen, 2006). I forbindelse med risiko kan dette føre til at mennesker konstruerer sin egen virkelighet, og vurderer risiko ut ifra sine egne subjektive persepsjoner. Innenfor samfunnsvitenskapelige tilnærminger til risiko omtaler man gjerne dette for opplevd risiko. Dette vil si at erfaringer, bakgrunn og informasjonsgrunnlag vil være med å påvirke hvordan risiko forstås og oppleves (Renn, 2008). I risikovurderinger for terrorhendelser, og tilsiktede handlinger generelt, vil risikopersepsjon spille en viktig rolle da man baserer seg på analytikernes kunnskap og erfaring, og mindre på empirisk data og statistikk. Solvic og Weber (2002) påstår at persepsjon og mispersepsjon i forbindelse med risiko, både fra befolkningen og fra myndighetspersoner, virker til å spille en stor rolle i forbindelse med risikostyring av terrorismetrusselen. Aven (2014) hevder at risikopersepsjonen inkluderer menneskers følelser, og kan ha innvirkning på hvorvidt man vurderer en hendelse som mulig, hvilke konsekvenser de kan få, sannsynligheter og usikkerhet samt akseptkriterier. Risikopersepsjon eller opplevd risiko er sammensatt, og det er viktig å fange opp det som strekker seg utover parameterne, som sannsynlighet og konsekvens, da det er langt flere faktorer som vil virke inn.

Fischhoff (2002) hevder at det både for vurdering og kommunikasjon av terrorisierisikoen er behov for å inkludere teorier fra atferdsvitenskapen. Selv om inkludering av atferdsteori legger til et nivå av kompleksitet til et allerede komplisert problem, hevder han at man med en kommunikasjonsplan hvor dette er fraværende både kan blende og bedra seg selv.

Fryktfaktorer

Fryktfaktorer defineres av Slovic og Weber (2002) som et viktig element innenfor hvordan lekfolk oppfatter risiko. Dette står, i følge dem, i motsetning til faktorer eksperter vurderer som viktig, som er nært knyttet til forventet tap. Relevante fryktfaktorer hevdes å være manglede kontroll, stort katastrofepotensiale, urettferdig fordeling av konsekvenser og oppfattelsen av at risikoen er økende og ikke lett å redusere. Andre faktorer som ser ut til å påvirke risikopersepsjon er hvorvidt den er kjent eller ukjent, observerbar eller ikke, om den er ny og i forbindelse med manifesteringen av konsekvenser (Kasperson, Pidgeon og Slovic, 2003).

Heuristikker og biaser

Heuristikker kan forklares som tommelfingerregler eller kognitive snarveier som vi benytter når vi skal vurdere og prosessere informasjon. Ved hjelp av heuristikker kan vi omgjøre komplekse problemer til enklere og mer overkommelige kognitive oppgaver (Kahneman, 2012).

Heuristikker kan dermed være behjelpelig med å ta gode nok beslutninger under visse situasjoner, men kan også skape et feilaktig bilde over situasjonen. Noen typiske heuristikker er:

Representativitet: Her vurderes sjansen for at noe er tilfellet, basert på hvor typiske de virker.

Tilgjengelighet: Bruk av tilgjengelighetsheuristikken innebærer at eksempler som er lett tilgjengelig i hukommelsen vurderes som mer sannsynlig enn eksempler som er mindre tilgjengelige. Dette gjør at hendelser som har skjedd nylig eller hendelser som har vært dramatiske eller spesielle huskes bedre enn dagligdagse hendelser.

Forankring og justering: Denne heuristikken henviser til at mennesker har en tendens til å justere gitte estimater og prediksjoner for lite når man får inn ny informasjon.

Heuristikker kan fungere som effektiviserende mentale verktøy når oppgaver blir for krevende, og løsningene kan ofte være gode nok. Når vi mennesker skal bedømme sannsynlighet og usikre situasjoner kan det oppstå biaser, eller beslutningsfeller. Dette innebærer systematiske avvik i forbindelse med normative logiske og statistiske regler (Eid og Johnsen, 2005).

Det å bli utsatt for et terrorangrep er kanskje ikke det mest tenkelige at skal skje når man går ut av huset om morgenen, men likevel hevder Rogers et al. (2007) at terrorisme er en stor bekymring blant befolkningen. De henviser til en undersøkelse, gjort i EU, som viste at trusselen om internasjonal terrorisme var den som var tilknyttet mest frykt til ut av ti ulike hendelser som kunne ha verdensomspennende katastrofale følger.

Analytikere som inntar den teknisk/naturvitenskapelige tilnærmingen til risiko vil gjerne oppfatte menneskers opplevde risiko som irrasjonelt og styrt av følelser. Innenfor denne tilnærmingen blir resultatet av risikoanalysene oppfattet som den reelle og objektive risikoen, og tanken er at om man gir befolkningen og lekfolk tilstrekkelig med kunnskap vil de også se den reelle risikoen. Dette står i motsetning til den bayesianske tilnærmingen, og Aven og Renns (2010) anbefaling om at målet med risikokommunikasjon ikke bør være å overbevise mennesker om at analytikeren sitter på det eneste riktige svaret. Den sistnevnte må argumenteres for at er

mest passende for den dynamiske terrorismerisikoen; den vil ikke være den samme for alle lokasjoner, verdiene som ønskes å beskytte er ikke de samme og å tro at man besitter det sanne svaret om framtidige terrorhendelser kan betraktes som uheldig og naivt.

For å bygge bro mellom det profesjonelle mandatet og offentlighetens risikopersepsjon er man avhengig av at toveiskommunikasjon finner sted mellom forskere, risikoledere, interessegrupper og representanter fra den berørte befolkningen. Renn (2004) mener denne dialogen bør inneholde tre viktige funksjoner: i) skape forståelse for forskjellige risikoperspektiver blant forskere, regulatorer, interessenter så vel som relevante deler av befolkningen. ii) opplyse alle disse partene om ulike rasjonale for å håndtere risiko, og iii) utvikle hensiktsmessige prosedyrer for konflikthåndtering.

Simonsen (2009) mener også det er viktig å ta hensyn til målgruppens oppfatning av risiko. Han hevder at ekspertene vil være mest opptatt av å formidle hvor liten sannsynlighet det er for at noe skal skje, mens befolkningen er opptatt av konsekvensene. Jo mer skremmende konsekvensene er jo høyere antas folks subjektive oppfatning av sannsynlighet for at en hendelse skal inntreffe å være (Simonsen, 2009).

6 Diskusjon

I dette kapitlet vil empiriske funn drøftes i lys av det teoretiske rammeverket introdusert i teorikapitlet. I første delkapittel vil de ulike definisjonene av risiko settes i en terrorismekontekst. Deretter vil de ulike tilnærmingene til risiko diskuteres ut fra hvorvidt de tar høyde for usikkerhet og risikopersepsjon. Delkapittel 6.2 retter fokus mot ulike måter å analysere risiko på, og hvilke implikasjoner dette kan medføre. Deretter vil det bli diskutert hvorvidt terrorismerisikoen kan framstilles visuelt. Til slutt blir det diskutert hvordan man kan kommunisere risiko uten å skape unødig frykt, og hvordan vi kan kommunisere det vi ikke vet.

6.1 Risikoforståelse

Her vil de ulike definisjonene og ulike tilnærmingene til risiko være hovedfokuset, og det vil vektlegges å redegjøre for hvilken risikoforståelse disse kan resultere i. Risikoforståelsen argumenteres i denne oppgaven som avgjørende for en forståelig og effektiv kommunikasjon av risikoer relatert til terrorisme.

6.1.1 Risikobegrepet i terrorismekontekst

Risiko knyttet til terrorisme, og tilsiktede handlinger generelt, skiller seg fra andre risikoer først og fremst fordi det finnes en kalkulert aktør med ondsinnede hensikter i den ene enden. Den skiller seg fra risikoer knyttet til naturhendelser og teknisk svikt ved at man ikke kan påvirke angriperen i like stor grad som man kan forbedre maskiner og forutse naturhendelser. For denne oppgaven er tre risikodefinsjoner valgt ut for å diskutere i hvilken grad de de fanger opp utfordringene i forbindelse med terrorismerisikoen. Grunnen til at det er disse som er valgt ut er at den første kan knyttes til NS 5814 og den teknisk/naturvitenskapelig tilnærmingen, den andre til den bayesianske tilnærmingen og den tredje til NS 583X-serien og trefaktortilnærmingen.

Risiko som sannsynlighet og konsekvens

I følge denne definisjonen av risiko vil resultatet av risikoanalysen beskrives kvantitativt i form av forventet verdi/tap. I en terrorismekontekst må sannsynlighetsfaktoren kunne dekke trusselaktørens hensikt, motivasjon og kapasitet. Dette er faktorer det er vanskelig å måle, og uten å uttrykke kunnskapen som ligger til grunn vil det være vanskelig å bedømme om en slik framstilling er korrekt. Konsekvenssiden må dekke mulige skader angriperen kan gjøre mot for eksempel liv, helse og materielle verdier. Det er også vanskelig å sette kvantitative verdier på en del av konsekvensene; det vil være mulig å se på bygningskonstruksjon for å se hvor stor skade en så eller så stor bombe vil gjøre. Det vil være mulig å få en statistisk oversikt over hvor mange mennesker som vanligvis befinner seg i et område eller i en bygning. Det vil imidlertid trolig være vanskelig å kunne fange opp konsekvenser som frykt, uro og eventuelle ettervirkninger. Med denne begrunnelsen er det vanskelig å se at dette skal være en gunstig måte å definere terrorismerisikoen i en risikovurdering. Framstillingen vil ikke fange opp alle kjennetegnene ved risikoen, og det vil trolig kunne bidra til feilaktig beslutningsgrunnlag for videre prioritering og håndtering. Det virker til å være stor enighet innen sikkerhetsforskningen om at en slik

formulering av risiko ikke er tilstrekkelig for risikoer som er befestet med stor usikkerhet (Jore og Njå, 2010; Aven et al., 2007; Renn, 2008 og Pettersen og Engen, 2010). På bakgrunn av etterspillene og Gjørsv-kommisjonenes rapport etter 22. juli kritiserer også Aven (2012) denne risikotenkningen som fullstendig foreldet. Dette nettopp fordi en slik tilnærming ikke i tilstrekkelig grad fanger opp kunnskaps- og usikkerhetsdimensjonen. Han mener at mange hendelser nedtones i risiko- og sårbarhetsanalyser fordi de kommer ut med en lav verdi av sannsynlighet og konsekvens, men at dette blir villedende og feil dersom kunnskapen er svak og usikkerhetene er store. Slovic og Weber (2002:5) hevder at store deler av samfunnsvitenskapen avviser en objektiv kvantifisering av risiko, og mener at en slik tilnærming i beste fall er ufullstendig og i verste fall villedende.

Risiko som konsekvenser og tilhørende usikkerhet

I denne definisjonen er ikke sannsynlighetsbegrepet eksplisitt med i definisjonen, men implisitt ligger bruk av kunnskapsbasert/subjektiv sannsynlighet som en måte å uttrykke usikkerheten knyttet til hvorvidt en hendelse vil inntreffe. I denne forståelsen av risiko vil også vurdering av styrken på bakgrunnskunnskapen spille en viktig rolle (Aven og Renn, 2010 og Aven, 2015). Det legges til grunn at vurderingen som gjøres av risikoen er subjektiv, som også vil si at resultatet fra vurderingen kan være forskjellig ut fra hvem som vurderer. Dette betyr ikke nødvendigvis at det ene er mer korrekt enn det andre, men gjenspeiler heller dynamikken som ligger i risiko. Det er ikke gitt at risikoen for terrorangrep vil være den samme for alle virksomheter, regioner eller objekter, og derfor er det også naturlig at risikoen vil få ulikt utfall og prioritering hos ulike aktører. Den viktigste faktoren her, som er fraværende i sannsynlighet/konsekvens-definisjonen, er et uttrykt behov for å redegjøre for og vurdere bakgrunnskunnskapen. Som nevnt i forrige avsnitt vil svakheter og usikkerhet i dette elementet lede til en høyere risiko.

Bruk av subjektiv sannsynlighet anbefales også i NS 5814:2008. Et forbedringspotensial i standarden, sett i forbindelse med Avens forståelse, er at risikoforståelsen må være bredere og inkludere usikkerhet og bakgrunnskunnskap.

Risiko som forholdet mellom trussel, verdi og sårbarhet

I et forsøk på å komme med et alternativt rammeverk, som spesifikt er tilpasset beskyttelse mot tilsiktede handlinger, velger NS 5830:2012 en risikodefinitjon som verken inkluderer sannsynlighet eller konsekvens. Fokuset her ligger på faktorene trussel, verdi og sårbarhet, og forholdet dem imellom. I definisjonen ligger det en slags rekkefølge på vurderingen hvor man ser på forholdet mellom trusselen mot en gitt verdi for og så se på forholdet mellom verdiens sårbarhet overfor den spesifikke trusselen. En del av kritikken mot sannsynlighetsbegrepet retter seg mot at det er en matematisk term, hvor tallfesting av risiko er påkrevd. Om målet med NS 5830:2012 er å gå bort fra denne utfordringen er det problematisk at de benytter "forholdet mellom" i sin definisjon. Busmundrud et al. (2015) hevder at dette ut i fra et naturvitenskapelig ståsted henviser til en matematisk operasjon, og i så måte må man kunne anta at problematikken med tallfesting av de ulike elementene også her vil være tilstede. Den matematiske operasjonen som "forholdet mellom" leder til vil være å dividere den første med den andre for å finne forholdet mellom størrelsene. Med denne framgangsmåten, og rekkefølgen i operasjonen

risikodefinsjonen maner til, vil resultatet av forholdet mellom trussel og sårbarhet bli feilaktig; høy sårbarhet vil nemlig gi lav risiko (Busmundrud et al., 2015:15). Selv om formuleringen av risikodefinsjonen er uheldig, må man likevel anta at det ikke er en slik operasjon de som har utarbeidet standardene (NS 583X-serien) henviser til, men heller viser til en lite gjennomtenkt formulering av begrepet.

Sammen med trefaktormodellen har også NS 5832:14 innført begrepet “ren risiko”. For terrorismerisikoen er det uklart hvor stort behovet er for denne avgrensningen. Det er vanskelig å se for seg at risikoen for tilsiktede handlinger vil kunne medføre gevinster, og terror er strengt tatt ikke forbundet med noen form for positiv gevinst, med unntak av fra angriperens side. Om målet var å vurdere sikringsrisikoen sammen med andre risikoer som kan være relevante for virksomheten kan avgrensningen ses på som gunstig for å skille mellom ulike typer konsekvenser. Men da NS 583X-serien retter seg spesifikt mot sikring for tilsiktede handlinger er det trolig ikke det som er hensikten.

6.1.2 Er terrorismerisikoen kompleks, usikker og tvetydig?

En viktig bekjennelse når en skal vurdere risiko er å kjenne sine egne begrensninger i forbindelse med informasjon og kunnskap. Ekspertvurderinger blir ofte benyttet for å få et mer helhetlig bilde og en større forståelse av de aktuelle risikoene. Renn (2008) introduserer “rulletrappmodellen” som et forslag til hvordan aktører som bør involveres i risikostyringsprosessen basert på usikkerheten, tvetydigheten og kompleksiteten til risikoen. Som vist i figur 3.3 øker antall anbefalte aktører i takt med usikkerhet, tvetydighet og kompleksitet. Dette uttales også som viktige karakteristikk for å avgjøre hvordan risikokommunikasjon skal tilrettelegges (OECD, 2002). Det anses derfor som nødvendig å drøfte i hvilken grad terrorismerisikoen kjennetegnes av disse faktorene.

Midtgård (2016) nevner at det er flere utilsiktede hendelser som viser seg å være mer komplekse enn de tilsiktede. På den ene siden er det rimelig å påpeke at det finnes hendelser med mer kompleksitet enn terrorhendelser. På den andre siden er det rimelig å heller snakke om grad av kompleksitet. Om enkelhet og kompleksitet betraktes som en dikotomi ville nok ikke terrorhendelser havne innenfor kategorien “enkel risiko”. Midtgård begrunner uttalelsen med at tilsiktede handlinger ikke i like stor grad vil få konsekvenser for kritiske samfunnsfunksjoner. Det er rimelig å argumentere for at dette ikke nødvendigvis alltid stemmer. For eksempel viste terrorhendelsen 22.juli at konsekvensene strakk seg langt utover tap av menneskeliv og materielle verdier. Blant annet var det et enormt trykk på telenettet som igjen førte til utfordringer i forbindelse med kommunikasjon mellom aktører i beredskapsinnsatsen. Man må også kunne forvente at terrorangrep kan ramme både bygg med symbolsk verdi og som har en funksjon i forbindelse med opprettholdelse av kritiske samfunnsfunksjoner.

Det er bred enighet om at det er tilknyttet stor usikkerhet til terrorismerisikoen (Hoffmann, 2016; Midtgård, 2016; Aven, 2015; Fishhoff, 2002; Renn, 2008; Jore og Njå, 2012; Weiss, 2007; DSB, 2014 og NSM, 2016). Det argumenteres videre for at denne usikkerheten er knyttet til analytikernes kunnskap, og at en mulig måte å identifisere usikkerheten på er å knytte den til

PSTs indikatorer for trusselvurdering: *tilstedeværelse, kapasitet, intensjon, historikk og målvalg* (Hoffmann, 2016).

Tvetydighet, slik det forstås i denne oppgaven, kan være gjeldene for terrorismerisikoen på to måter, i forbindelse med både fortolkende og normativ tvetydighet. Fortolkende tvetydighet er relatert til at de som analyserer risikoen ikke er enig om hvorvidt den informasjonen man innehar tilsier at risikoen er høy eller lav. Altså oppstår det uenighet i forbindelse med ”bevismaterialet”. Normativ tvetydighet oppstår når man er uenig om verdiene, men enig om ”bevismaterialet”.

Terrorismerisikoen vil da kunne relateres til kompleksitet, usikkerhet og tvetydighet. Dette fordrer, i følge Renns rulletrappmodell (figur 3.3) og OECDs råd at man i vurdering av risikoen må ta med representanter av sivilbefolkningen, relevante/berørte interessenter, forskere og ansatte i virksomheten. Det må bemerkes at det ikke nødvendigvis er terrorhendelser verken OECD (2002) eller Renn (2008) refererer til, men risikokarakteristikkene som defineres må kunne sies å stemme for risikoen relatert til terrorhendelser. Det som er en utfordring med vurderinger og analyse av terrortrusselen, og en utfordring med å implementere Renns modell for involvering av interessenter, er at vurderingene som regel er basert på sikkerhetsgradert informasjon. Dette hindrer innsyn for folk flest, noe som betyr at det er begrenset hvem som kan være med i vurderings- og analyseprosessen på nasjonalt nivå. Det er derfor nærliggende å anta at informasjonsutveksling og samarbeid i forbindelse med trusselvurderinger, hos aktører som PST, i beste fall foregår innad i organisasjonen og med lignende organisasjoner i andre land, og innad i Norge. DSB har en annen innretning hvor de søker å gjøre all informasjon brukt i NRB ugradert, og dermed tilgjengelig for alle (Midtgård, 2016). På den ene siden er dette en fordel da all informasjonen blir tilgjengelig for alle som har behov for å ta høyde for risikoen. På den andre siden er det rimelig å stille spørsmål om all informasjon faktisk blir formidlet da også analysene i NRB er basert på informasjon fra PST. I så tilfelle vil man gi inntrykk av at den tilgjengelige informasjon er kommunisert, men i virkeligheten holder tilbake informasjon som er sikkerhetsgradert.

6.1.3 Risikotilnærming og kommunikasjon av terrorismerisiko

De ulike tilnærmingene til risiko legger føringer for hvordan risikoen styres og vurderes (Aven et al., 2004; Renn, 2008 og NSM, 2016). Det argumenteres også for at tilnærmingen til risiko legger føringer for hvordan risiko kommuniseres. Det vil derfor i dette delkapitlet diskuteres hvorvidt de ulike tilnærmingene – teknisk/naturvitenskapelig-, bayesiansk- og trefaktortilnærmingen – kommuniserer terrorismerisikoen. Dette basert på om usikkerhetene kommuniseres, hvem som potensielt kan involveres i prosessen og hvorvidt det blir tatt høyde for opplevd risiko.

6.1.3.1 Teknisk/naturvitenskapelig tilnærming

Den tradisjonelle måten å se på risiko er å vurdere sannsynlighet i kombinasjon med konsekvens, og deretter styre implementeringen av årsaks- og konsekvensreducerende tiltak etter de gitte resultatene. I dette perspektivet legges det til grunn at sannsynlighet og konsekvens

er objektive størrelser, og at det dermed er mulig å komme fram til en sann risiko. Resultatet av risikovurderingen er gjerne basert på statistikk og historiske data. For en rekke hendelser hvor det foreligger tilstrekkelig med data kan dette være en hensiktsmessig del av risikovurderingen, men som enkeltstående tilnærming har den sine klare begrensninger. Eksempelvis kan dette være en god måte å vurdere antall trafikkulykker ved å se på antall ulykker og konsekvensomfanget, for å kunne si noe om forventet antall drepte i trafikken i de kommende årene. Det finnes blant annet statistikk på hvilke dager det er “farligst” å kjøre på og hvilke veistrekninger som er mest utsatt. En slik vurdering kan gi indikasjoner i forbindelse med implementering av tiltak som veidelere, informasjonskampanjer og flere kontroller. Det en slik vurdering imidlertid ikke vil gi informasjon om er hvor hendelsene vil inntreffe, hvor mange som vil være involvert og tidspunkt for ulykken.

Det er vanskelig å se at en slik tilnærming til risiko skal være tilstrekkelig for å vurdere og kommunisere terrorisierisikoen. Beskrivelsen av forskjellen mellom safety- og security-relaterte risikoer viser at det som skiller dem er at tilsiktede handlinger er planlagte og viljestyrte hvor trusselaktøren handler målrettet. Trusselaktørene er rasjonelle, kalkulerende, fleksible og tilpassningsdyktige individer (Albrechtsen, 2003; Aven, 2014 og Hoffman, 2006). Trusselaktøren forsøker ved hver hendelse å skremme og overraske, og man kan dermed beskrive terrorisierisikoen som uforutsigbar (Aven, 2014). Disse kjennetegnene, i tillegg til at det finnes lite empirisk data og at hendelsene ikke er gjentakende, gjør at det er utfordrende å se på hvilken måte man kan fastsette objektive verdier på de faktorene som påvirker risikoen. Ved å legge en frekvensbasert tilnærming til grunn for vurdering av terrorisierisikoen vil mange viktige elementer overses, og med manglende tidligere hendelser vil en utregnet risiko ikke gi mye mening. I tillegg argumenteres det for at uventede og ekstreme hendelser vanskelig vil la seg fange opp med en tilnærming hvor man baserer seg på historisk data og statistikk.

Albrechtsen (2003) framhever også at security-hendelser er preget av mer usikkerhet enn safety-hendelser, og denne usikkerheten ligger i all hovedsak i etterretningen og analytikernes kunnskap. Dette er informasjon som raskt kan endre seg og dermed endre risikonivået. I tillegg er også informasjon noe som er vanskelig å tallfeste, og dermed vanskelig å inkludere i en matematisk formel på risiko. Framstilling av en objektiv verdi på risiko tilsier også at usikkerhetselementet er håndtert, og at resultatet er fakta. Det at ny informasjon har mye å si for resultatets validitet vil si at terrorisierisikoen er dynamisk, og ikke statisk. Hvis en matematisk framstilling av terrorisierisikoen skulle ha noe for seg måtte dette tallet oppdateres kontinuerlig etter hvert som det kom ny informasjon. En kan også stille spørsmålsteget om objektive tall på risiko, presentert av en ekspertgruppe, vil oppfattes som tilstrekkelig og pålitelig av offentligheten.

Når det gjelder kommunikasjon av terrorisierisikoen innenfor denne tilnærmingen er det utfordrende å argumentere for at den skal være tilstrekkelig. Frekvensbaserte sannsynligheter uttrykker aleatorisk usikkerhet, men ikke den epistemiske knyttet til analytikerens bakgrunnskunnskap. Siden lekfolks opplevde risiko innenfor denne tilnærmingen oppfattes som irrasjonelt og følelsesstyrt vil nok heller ikke risikopersepsjon og atferdsteori bli tatt høyde for. En frekvensbasert sannsynlighet for et terrorangrep, i Norge for eksempel, ville trolig vært lik

null om tallet skulle baseres på statistikk på tidligere hendelser. Det er nærliggende å anta at en slik vurdering ville blitt feil, men det som er mest problematisk er at en slik framstilling ikke får fram det viktigste, nemlig usikkerheten. Det er også vanskelig å se for seg at det går å sette en nasjonal verdi på terrorismerisikoen, da det ikke nødvendigvis vil være like stor fare for et angrep over hele landet.

I denne oppgaven argumenteres det for at historisk data og statistikk kan bidra til økt forståelse for fenomenet terror, og virkemidler som har vært brukt i tidligere angrep. Imidlertid er det viktig å ta høyde for at trusselaktøren er en kalkulerende og strategisk person, som i tillegg er tilpasningsdyktig både i forbindelse med implementerte tiltak og bruk av nye metoder. Frekvensbaserte sannsynligheter blir dermed betraktet som utilstrekkelig for å kommunisere terrorismerisikoen.

6.1.3.2 Bayesiansk tilnærming

Den samfunnsvitenskapelige tilnærmingen til risiko skiller seg fra den naturvitenskapelige ved at den hensynstar menneskers risikopersepsjon (Aven et al., 2004). Dette kan sies å være det viktigste bidraget fra den samfunnsvitenskapelige tilnærmingen som er tatt med inn i den bayesianske tilnærmingen.

Både den naturvitenskapelige og samfunnsvitenskapelige tilnærmingen har, i følge Aven et al. (2004), sine begrensninger, og den bayesianske tilnærmingen foreslås som en brobygger mellom de to tilnærmingene. Den bayesianske tilnærmingen, i forbindelse med vurdering av terrorismerisikoen, anbefales også av Jore og Njå (2010). Aven (2003) hevder at det i denne tilnærmingen ikke er en skarp forskjell mellom objektiv og opplevd risiko; risiko er en vurdering, ikke fakta. Dette betyr at risikoanalytikerer ikke har enerett til å definere risiko, men at det kan ses på som et bidrag til økt forståelse og beslutningsstøtte. I risikoanalyser gjennomført i henhold til den bayesianske tilnærmingen vil fokuset være på de observerbare dataene, som for eksempel terrorhendelser mot en spesifikk del av kritisk infrastruktur i året som har gått (Jore og Njå, 2010). Dataen her vil være usikker i tidspunktet analysen gjennomføres, men vil bli kjent i framtiden. Ingen innehar fullstendig kunnskap om framtiden, og kan derfor aldri predikere den med 100 % sikkerhet. Usikkerheten kan her uttrykkes med subjektive sannsynligheter. Forskjellen fra sannsynligheter brukt i den teknisk/naturvitenskapelige tilnærmingen, som har til hensikt å beskrive en objektiv verdi, er at sannsynlighetene her tar forbehold om analytikerens begrensninger i bakgrunnskunnskapen (Jore og Njå, 2010). Dette legger videre føringer for at bakgrunnskunnskapen må granskes da den legger føringer for evalueringen av risiko.

Befolkningens frykt og meninger angående risiko anses ut i fra den naturvitenskapelige tilnærmingen som irrasjonelle (Aven et al., 2004). Fra den bayesianske tilnærmingen anses derimot dette som et viktig aspekt å inkludere når det skal vurderes hvorvidt risikoen kan aksepteres, og på hvilken måte den kan håndteres. Årsaksreducerende barrierer for terrorisme kan ofte gå på bekostning av andre verdier vi mennesker verdsetter høyt, som åpenhet, frihet og demokrati. I slike situasjoner vil kartlegging av befolkningens risikopersepsjon kunne fungere som et bidrag i veiingen av fordeler og ulemper med håndtering av risiko. En kjent

misoppfatning angående risiko er at mennesker er mer redd for å kjøre bil enn å fly, enda det statistisk sett er langt farligere å kjøre bil enn å fly. Dette forklares via psykologiske teorier ut i fra såkalte fryktfaktorer, som at mennesker frykter det ukjente mer enn det kjente. I tillegg er kontrollerbarhet, frivillig eksponering og risikoforståelse faktorer som påvirker menneskers risikopersepsjon (Kasperson, Pidgeon og Slovic, 2003). På denne siden kan inkludering av menneskers oppfatninger angående risiko gi en pekepinn på hva som bør kommuniseres og formidles for å gi befolkningen en best mulig forståelse av risikoens natur og omfang.

Aven og Renn (2010) foreslår at risikoen beskrives og at usikkerheten uttrykkes. Om dette tolkes dithen at det er tilstrekkelig med kun sannsynlighetsangivelser for usikkerheten, og ingen beskrivelse av bakgrunnskunnskapen, anses ikke dette som tilstrekkelig. Om det derimot, slik som Aven (2015) anbefaler, redegjøres for bakgrunnskunnskapen i tillegg til sannsynlighetene vurderes dette som en hensiktsmessig måte å framstille terrorisierisikoen.

Den bayesianske tilnærmingen er den som er mest forenlig med DSBs tilnærming, hvor den benyttes for både tilsiktede handlinger og utilsiktede hendelser i deres nasjonale risikobilde.

6.1.3.3 Trefaktortilnærmingen

Trefaktortilnærmingen til risiko er det nyeste bidraget som blir diskutert i denne studien. Den største akademiske utfordringen med denne tilnærmingen er at den ikke har den samme vitenskapelige forankringen som de andre tilnærmingene. Dette kan, på den ene siden, til dels forsvares ved at det er et relativt nytt bidrag. På den andre siden har det bydd på utfordringer med å gi en like klar beskrivelse av hva de legger til grunn for sine definisjoner og sin tilnærming. Trefaktortilnærmingen er forenlig med risikotilnærmingen til både NSM og PST.

Busmundrud et al. (2015) virker å være enig angående det vitenskapelige grunnlaget, og hevder at den såkalte trefaktormodellen ikke har den samme brede teoretiske forankringen som NS 5814:2008. De mener at tilnærmingen bærer preg av at det teoretiske rammeverket kom på plass i etterkant av utformingen av trefaktormodellen. Dette er i så tilfelle uheldig da det kan tenkes at de da har lett etter teorier som bekrefter sine forutinntatte betraktninger, og dermed kan ha nedprioritert å sette seg inn i forskningen innenfor fagfeltet. Det vurderes blant annet at deres syn på sannsynlighet, som en utelukkende kvantitativ og matematisk formel, kan være et bevis på at nyere og viktige bidrag i risiko- og sikkerhetsforskningen er oversett. Barane (2014) forsvaret det teoretiske grunnlaget til trefaktortilnærmingen. Han hevder rammeverket for sikringsrisikostyring er forankret i samfunnsvitenskapen og er basert på teorier fra blant annet kriminologi, sosiologi og psykologi. Han forklarer at det teoretiske fundamentet baserer seg på blant annet teorien om rasjonelle valg, rutineaktivitetsteorien og APT-teorien (se s. 25).

Rammeverket tilknyttet trefaktormodellen legger ingen spesifikke føringer for hvem som bør være med i analyseprosessen (NSM, 2016; NS 5831-2, 2014 og NSM, POD og PST, 2015). I sistnevnte blir det anbefalt at man kan søke ekspertise eksternt om virksomheten mangler kompetanse innad, men det legges ingen føringer for inkludering av risikopersepsjon eller opplevd risiko. I NS 583X-serien defineres sikkerhet som "*reell eller oppfattet tilstand av sikkerhet som innebærer fraværet av uønskede hendelser, frykt eller fare*" (NSM, POD og PST,

2015:9). Dette kan tolkes som at de innenfor denne tilnærmingen oppfatter risiko som noe objektivt, og at eksperter har en form for enerett i bestemmelser angående risiko. Definisjonen av sikkerhet er også misvisende da den, sammen med risiko, framstår som en dikotomi. Det tolkes da dithen at man ikke kan snakke om grad av sikkerhet eller risiko. Samtidig kan det argumenteres for at sikkerhet, slik de definerer det, er en uoppnåelig tilstand da det er vanskelig å se for seg en tilstand hvor det ikke vil finnes noen risiko.

Tabell 6.1 Oppsummering av de ulike tilnærmingene.

Risikotilnærming	Parametere	Eksperters resultater	Lekfolks opplevelse	Kommuniserer usikkerhet for terrorisierisikoen
Teknisk/naturvitenskapelig	Sannsynlighet og konsekvens	Objektiv sannhet	Irrasjonelle og følelsesstyrt	Nei
Bayesiansk/kunnskapsbasert	Konsekvenser og usikkerhet	Subjektiv vurdering	Relevant	Ja
Trefaktor	Verdi, trussel og sårbarhet	Objektiv sannhet	Ikke tatt høyde for	Nei

6.2 Risikoanalyse: samme formål og ulike resultater?

I teorikapitlet ble risikoanalyse beskrevet som en analyse av årsaker og konsekvenser og sammenhengen mellom disse. Selv om analysene baserer seg på ulike parametere er målet med risikoanalyse å identifisere trusler som kan true virksomheten, objektet eller systemet som undersøkes, og ut fra dette kunne ta informerte beslutninger angående hvilke tiltak som er nødvendig (Aven, 2007 og NSM, 2016). Det blir dermed avgjørende at beslutningsgrunnlaget blir formidlet av analytikerne og forstås av beslutningstakerne. For analyseobjektet er det sannsynligvis flere aktuelle risikoer, og en del av beslutningene gjelder prioriteringer av hvilke risikoer som kan aksepteres og hvilke som må håndteres med forebyggende og/eller konsekvensreducerende tiltak.

Konsekvensene som vurderes virker å være standardiserte for de fleste risikoanalyser, hvor tap av liv og helse, skader på miljø og tap av materielle verdier defineres som de viktigste. Det kan i så måte sies at risikoanalyser, uansett hvilken standard eller teoretisk rammeverk de baserer seg på, omhandler en form for trussel-, verdi- og sårbarhetsvurdering. Det som skiller trefaktormodellen fra både sannsynlighet- og konsekvenstilnærmingen og konsekvens- og usikkerhetstilnærmingen er at den ikke, hvert fall eksplisitt, vurderer sannsynligheten eller muligheten for at en hendelse skal inntreffe. Når trefaktormodellen ble introdusert og sannsynlighetsbegrepet ble etterspurt ble det forsvart med at bruk av parameterne sannsynlighet og konsekvens ville kunne lede til at risikoen fikk en lav score, og dermed ikke ble prioritert (Barane, 2014 og Olsen, 2013). Dette fordi sannsynlighetsvurderingen antas å dra ned den samlede risikoverdien. Om ikke usikkerhet er med som faktor her, kan begrunnelsen ses som rimelig. Om man derimot tar usikkerhet med i betraktning vil risikoer med høy usikkerhet og svak bakgrunnskunnskap øke risikoverdien, og for eksempel plassere den høyere opp i risikomatriksen og dermed prioriteringslisten (Aven, 2015).

I denne oppgaven argumenteres det for at, på samme måte som sannsynlighet kan dra ned risikoverdien på feilaktig måte, kan manglende bruk lede til at risikoen blir framstilt med feilaktig høy verdi. Tap av liv er den verste konsekvensen, og det som verdsettes høyest, i en risikoanalyse. Hvis vi tenker oss at dette er sett på som en av de mulige konsekvensene en risiko kan medføre vil trolig risikoen få en høy score i utgangspunktet. Om man da ikke gjennomfører en vurdering av hvor trolig det er at hendelsen skal inntreffe er det nærliggende å anta at alle risikoene som kan medføre tap av liv og helse presenteres som høye. Trefaktormodellen gir heller ingen eksplisitt forklaring på hvordan usikkerhet håndteres eller framstilles, og i kombinasjon med manglende sannsynlighet/mulighetsvurdering anses dette som uheldig. Det er også vanskelig å tenke seg at det ikke gjennomføres noen form for sannsynlighetsvurdering; i det man velger bort et scenario eller legger til ett i risikoanalysen har man jo i så måte gjort en vurdering om hvorvidt man kan tenke seg at scenarioet kan skje. Det kan kanskje heller være rimelig å stille spørsmålstegn ved hvorfor denne vurderingen ikke synliggjøres og kommuniseres.

En av årsakene til at analytikere innenfor security-feltet motsetter seg bruken av sannsynlighet for terrorhendelser kan tenkes å være den tilknytningen det har til risikohåndteringen. Det vil si at om man for eksempel setter en høy sannsynlighet for et angrep så følger gjerne implementering av hensiktsmessige beskyttelsestiltak. Disse tiltakene vil videre gjøre det mindre attraktivt for en potensiell angriper å angripe dette objektet, og sannsynligheten vil dermed reduseres. Et slikt eksempel illustrerer hvor viktig det er å formidle bakgrunnskunnskapen subjektive sannsynligheter baserer seg på, samtidig som at det understreker viktigheten med kontinuitet i risikostyringsprosessen.

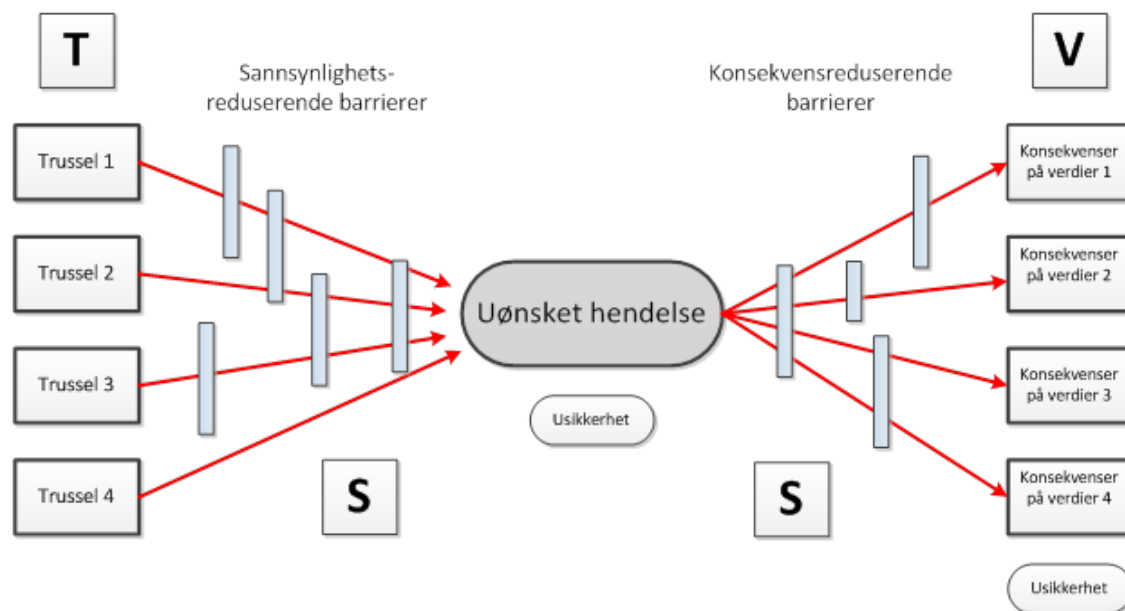
Det som oppfattes som mest problematisk med innføringen av trefaktortilnærmingen er at den virker som den er ment å erstatte den teknisk/naturvitenskapelige tilnærmingen, uten å ha tatt høyde for nyere bidrag innenfor sikkerhetsfaget. Om den bayesianske tilnærmingen, og dens fokus på usikkerhet og subjektive/kunnskapsbaserte vurderinger hadde blitt tatt med i prosessen, antas det at enigheten om hvilke metoder som skal brukes innenfor vurdering av sikringsrisiko hadde vært større. En felles språkdrakt og like metoder ville definitivt gjort det enklere å unngå misforståelser og feiltolkninger i kommunikasjon av risiko for terrorhendelser.

6.3 Kan terroriserisikoen framstilles visuelt?

Ulike framstillingsverktøy ble beskrevet i kapittel 3.4.3 Det som er viktig å understreke er at det i følge standardene kun er risikomatriksen (NS 5814) og risikotrekanten (NS 5832) som er anbefalte verktøy for å framstille de analyserte risikoene. Risikotrekanten anses som lite hensiktsmessig å sammenligne med risikomatriksen da de ikke kommuniserer det samme. For det første baserer de seg på ulike parametere. For det andre presenterer risikotrekanten én samlet risiko, mens risikomatriksen presenterer alle risikoene som er vurdert, og gir dermed mulighet til å sammenligne og prioritere. På bakgrunn av dette anses det mer rimelig å sammenligne risikotrekanten med andre anerkjente og mer informative analyseverktøy, som bow tie-diagrammet, feiltre og hendelsestre.

Risikotrekanten er et verktøy som intuitivt kun sier noe om hvilke parametere som er vurdert. Om den framstilles som vist i figur 3.9 kan reduksjon av risiko ved implementerte tiltak illustreres (NSM, POD og PST, 2015). Imidlertid viser figuren kun at risikoen er blitt lavere, den viser ikke *hva* som er gjennomført for at den er blitt det. På den ene siden kan det argumenteres for at dette er svært lite informativt. På den andre siden retter dette mer fokus på risikoanalysen og risikobeskrivelsen; for å kunne ta informerte beslutninger angående relevante risikoer er det jo tross alt dette som er viktig å sette seg inn i og forstå. Om trekantmodellen kun skal betraktes som et analyseverktøy kan det imidlertid argumenteres for at flere andre anerkjente analyseverktøy viser risikoen på en langt mer informativ måte. For eksempel vil feiltre- og hendelsestre kunne gi en visuell beskrivelse av årsaks- og konsekvenssammenhenger. Begge er også gunstige for å kommunisere hvilke barrierer som finnes og hvilken effekt de kan ha. Som nevnt kan begge disse også gjennomføres kvalitativt (Aven, Wiencke og Røed, 2008), og forutsetter ikke kompliserte matematiske kvantifiseringer av verdiene for å gi en god beskrivelse.

Der hvor feiltre- og hendelsestreanalyser tar for seg hver sin parameter av risikoen, sannsynlighet og konsekvens, har bow tie-diagrammet fordelen med at hele risikobildet kan framstilles i én figur. I følge DSBs illustrasjon av et bow tie-diagram (figur 3.4) er det heller ingen problem å også formidle usikkerheten. Dette gjøres for den uønskede hendelsen og for konsekvensene. Det vurderes heller ikke som umulig å benytte denne risikoframstillingen som et alternativ for risikotrekanten; hvor de medvirkende faktorene som fører til en uønsket hendelse representerer trusselen; konsekvensene som representerer verdiene; og til slutt de årsaks- og konsekvensreducerende barrierene som illustrerer sårbarheten (se figur 6.1). På denne måten kan fortsatt risikovurderingen basere seg på de tre parameterne verdi, trussel og sårbarhet, samtidig som hva som faktisk er vurdert kommer fram på en tydeligere måte.



Figur 6.1 Visualisering av risiko i bow-tie basert på trefaktormodellen.

I denne oppgaven vurderes ikke risikomatriksen som et alternativt framstillingsverktøy til noen av de ovennevnte analyseverktøyene, men anbefales som et supplement til samtlige, også risikotrekanten. Hver av de diskuterte analyseverktøyene – feiltre, hendelsestre, bow-tie og trefaktor – må vises for hver av risikoene som er vurdert, mens risikomatriksen viser en sammenstilling av alle. Dette gir muligheten til å ta beslutninger angående hvilke risikoer som må prioriteres og hvilke som kan aksepteres. En av utfordringene med risikomatriksen kan tenkes å være at den tillegges for mye vekt i beslutningsprosessen, og at den betraktes som selve risikoanalysen. Dette blir feil, og det er viktig å formidle at det kun er en sammenstilling av resultatene fra en langt mer inngående analyse.

Som vist i kapittel 3.4.3 (figur 3.6, 3.7 og 3.8) finnes det flere ulike måter å utforme risikomatriker. Når risikomatriksen benyttes er det også viktig å formidle hva den faktisk sier, og hva som er undersøkt. De to første figurene (3.6 og 3.7) viser sannsynlighet og konsekvens, mens den tredje (3.8) også inkluderer usikkerhet. Risikomatriksene fra DSB er også utformet på bakgrunn av scenarioer, og utfallet i risikomatriksen viser da ikke sannsynligheten for en terrorhendelse generelt, men sannsynligheten for det scenarioet de har undersøkt. Dette burde redegjøres i beskrivelsen, slik at det framkommer tydelig hva resultatet er basert på. Selv om DSB benytter farger for å formidle usikkerhet for scenarioene sier ikke risikomatriksen noe om hvilken innvirkning usikkerheten har hatt på plasseringen i matrisen. Det vil derfor argumenteres for at risikomatriksen, og de andre beskrevne framstillingsverktøyene, ikke er tilstrekkelig alene, men trenger en nærmere beskrivelse i tillegg.

6.4 Kommunisere risiko uten å bidra til unødig frykt

I analysekapitlet ble elementene ord- og tallforståelse, tillit og hensyn til atferd og frykt identifisert som sentrale hensyn å ta høyde for i kommunikasjon av risiko, særlig knyttet til terrorisme. I dette delkapitlet vil dette ses opp mot målet med risikokommunikasjon og foregående funn i diskusjonen.

Ulike fryktfaktorer defineres som viktige elementer innenfor hvordan lekfolk oppfatter risiko, og dette står i følge Slovic og Weber (2002) i motsetning til faktorer eksperter vurderer som viktig. Dette understreker viktigheten med å ta hensyn til atferdsteori og risikopersepsjon i risikokommunikasjon, og kjenne til hvilke faktorer som kan skape mer frykt enn andre. Når det gjelder hendelser som skiller seg fra dagligdagse hendelser, og som kjennetegnes av manglende kontroll, stort katastrofepotensiale, hvorvidt den er kjent eller ukjent og observerbar eller ikke vil påvirke menneskers frykt (Slovic og Weber, 2002 og Kasperson, Pidgeon og Slovic, 2003). I kombinasjon med at all informasjon sannsynligvis ikke er kjent for analytikeren heller, kan det være vanskelig å gi tilstrekkelig informasjon slik at man utelukker fryktfaktorer. Imidlertid er det rimelig å argumentere for at dette bør være kjente elementer for de som kommuniserer slik at de bedre kan forstå tilhørernes reaksjoner og handlemåter.

Kommunikasjon av risiko generelt, og terrorisierisiko spesielt, innebærer ofte at usikker og ufullstendig informasjon må formidles, både til beslutningstakere og befolkningen. I tillegg til å

gi tilstrekkelig informasjon, skal det i kommunikasjonsprosessen sørges for å skape og opprettholde tillit og samtidig ta høyde for at ulike tilhørere kan oppfatte meldingen forskjellig. Det sier seg selv at dette ikke er noen enkel oppgave, og det krever god planlegging for å få til.

Terrorismerisikoen er ikke tilknyttet et spesifikt system, et objekt eller en lokasjon. I den globaliserte verden vi lever i dag vil også hendelser som skjer i nærliggende land, og til og med på andre siden av verden kunne få innvirkning på utførte risikovurderinger (Aven, 2014). Det betyr ikke nødvendigvis at risikoen øker, men hendelsene får ofte stor oppmerksomhet både hos media og befolkningen, og skaper dermed et behov for informasjon fra ansvarlige aktører. I slike tilfeller vil det være behov for å informere om hva som blir gjort og hvordan dette påvirker beredskapsnivået i Norge. Dette gjelder befolkningen så vel som utsatte virksomheter. I kapittel 6.1 ble en frekvensbasert tilnærming til risiko diskutert, og dette ble sett på som en for smal tilnærming til terrorismerisiko begrunnet med at den ikke, i tilstrekkelig grad, fanget opp dynamikken i risikoen. Aleatorisk usikkerhet uttrykt med frekvensbaserte sannsynligheter vil kreve at variasjonen beskrives ut i fra estimer, og modelleres ved hjelp av sannsynlighetsmodeller. Frekvensbaserte sannsynligheter baserer seg på statistikk og tidligere erfaring, og en kan spørre seg hvor relevant dette er for terrortrusselen. Selv om nærliggende terrorhendelser, både i tid og rom, kan føre til frykt og uro blant befolkningen, samt økt oppmerksomheten rundt emnet fra myndighetene, er det ikke dermed sagt at sannsynligheten for et angrep øker.

Jenkins, Willis og Han (2016) har undersøkt i hvilken grad signifikante terrorangrep øker risikoen for flere angrep. Det som er et interessant funn å diskutere er at visse dager hvor store folkemengder typisk samles er spesielt utsatt. I denne forbindelse er det rimelig å argumentere for at arrangementer på slike dager har tatt forhåndsregler med hensiktsmessige sikringstiltak, og at man dermed kan vurdere sannsynligheten for et angrep som lavere. Samtidig betyr ikke dette at sannsynligheten for et angrep generelt har gått ned, da trusselaktøren har mulighet til å endre lokasjon for angrepet. Dette kan ses i sammenheng med bombingene av regjeringskvartalet 22. juli, hvor det i ettertid var diskusjoner om hvorvidt stenging av Grubbegata kunne avverget angrepet. Potensielt sett så kunne det nok det, men det er også rimelig å anta at målet til angriperen kunne blitt endret, og bombingene kunne skjedd ved en annen lokasjon. Dette er et viktig dilemma som både må formidles fra analytikerne og tas høyde for av beslutningstakerne. Virksomheter som beslutter å sette inn sikringstiltak på steder de anser som sårbare må være bevisst på at sårbarheten i så måte kan endre plass. Her kan man stille seg spørsmålet om det i det hele tatt er vits å sikre for terror eller om vi skal sette i gang sterkere og mer omfattende terrorsikringstiltak? I denne oppgaven forblir dette spørsmålet ubesvart, da det faller utenfor rammene av oppgaven. De bakeforeliggende vurderingene for sikringstiltak anses likevel som viktig å formidle og forstå.

Risikopersepsjon refereres til som en mental prosess hvor mennesker tar inn, håndterer og vurderer informasjon fra omgivelsene. I forbindelse med risiko vil dette si at man kan konstruere sin egen virkelighet, og at dette gjøres ut fra subjektive vurderinger basert på egne erfaringer, bakgrunn og kunnskap (Renn, 2008 og Aven, 2014). Heuristikker kan være gunstig å se på når man skal kartlegge hvordan mennesker prosesserer og vurderer informasjon, men

også hvordan de noen ganger kan føre til mistolkning av situasjonen (Kahneman, 2012). Heuristikker som kan være relevante å diskutere er blant annet tilgjengelighet, hvor man betrakter eksempler som er lett tilgjengelig i hukommelsen som mer sannsynlige enn de som ikke er det (Kahneman, 2012). En av betraktningene om terrorhendelser er, som sagt, at de skaper frykt. Hendelser relatert til terror er kontroversielle og får gjerne stor oppmerksomhet i media, hos myndighetspersoner og hos befolkningen generelt. Dette gjør at vi husker disse hendelsene ekstra godt, og Kahneman (2012) hevder at dette kan gjøre at vi også tenker at disse hendelsene er mer sannsynlig at skal inntreffe. Andre hendelser som typisk kan tenkes å påvirke oss i samme retning er om det inntreffer en flyulykke. Etter en flyulykke vil kanskje enkelte passasjerer være mer redd for å fly, selv om det, logisk sett, er sannsynlig at operatørene i flybransjen er ekstra påpasselige etter at det har vært en ulykke.

Forankring- og justeringsheuristikken kan også sies å være relevant. Her dreier det seg om hvorvidt man justerer sine valg etter et gitt estimat. Kahneman (2012) mener at man har en tendens til å legge for stor vekt på det foreslåtte estimatet, og justerer det for lite i etterkant. Dette kan for eksempel ha betydning i forbindelse med hvor mye vekt som legges på andre sine vurderinger når man skal forme sine egne analyser. Her vil det være viktig å presisere at risikovurderinger er subjektive, og det er derfor viktig å basere risikoanalyser og på faktorer som er relevante for sin egen virksomhet, og ikke kopiere sannsynlighets-, konsekvens- og usikkerhetsvurdering fra andre analyser. Det vil for eksempel ikke gi mye mening å kopiere scenarioene analysert i NRB til verken virksomheter, fylker eller kommuner uten å vurdere relevansen det har for det som faktisk vurderes.

Det er verdt å nevne at det kan være problematisk å diskutere heuristikker i forbindelse med risiko innenfor en subjektivistisk tilnærming til risiko. Dette begrunnet med at heuristikker i så måte kan gi inntrykk av at det finnes sanne verdier på risiko, men at mennesker ikke oppfatter dem.

6.5 Hvordan kan vi kommunisere det vi ikke vet?

Hovedutfordringen med å kommunisere risiko relatert til terrorhendelser kan sies å være det faktum at man må kommunisere det man ikke vet. I det øyeblikket all informasjon om et angrep er tilgjengelig, om den blir det, er angrepet gjerne forhindret eller gjennomført. Ved den økte terrortrusselen, med påfølgende forhøyet beredskapsnivå, sommeren 2014 uttalte PST: *“Det foreligger en konkret og tidsavgrenset terrortrussel mot Norge. ... hvem som står bak, hva målet eventuelt er og hvordan et eventuelt angrep skal gjennomføres, er ikke kjent”* (Lilleåsen, 2014). Dette var informasjon som både påvirket den nasjonale beredskapen, enkelte virksomheters og arrangementers beredskap samt skapte uro blant befolkningen. Man kan spørre seg om det er riktig å gå ut med slik informasjon offentlig. På den ene siden kan usikkerheten knyttet til meldingen skape unødig frykt og uro blant befolkningen, og skape mistillit ved at man tror at den som informerer tilbakeholder informasjon. På den andre siden førte terrortrusselen sommeren 2014 til økt synlig beredskap (Bjørnland, 2014a), som bevæpnet politi, økt vakthold og strengere grensekontroll, som uten informasjon trolig kunne skapt enda mer frykt og uro. En

del av tillitsaspektet, og et av målene med risikokommunikasjon er å forsikre tilhørerne om at ansvarlige aktører håndterer situasjonen med de midler som er nødvendig (Aven og Renn, 2010 og Rogers et al., 2007) hevder at dette er særlig viktig når det gjelder nasjonal sikkerhet og kontraterrorisme. Det er også verdt å nevne at dette var en akutt situasjon, og disse utfordringene vil ikke i like stor grad være gjeldende for vanlige risikoanalyser. I akutte situasjoner, som den økte terrortrusselen sommeren 2014, vil det være mange som har noe å si. Det er eksperter som uttaler seg, andre eksperter som tolker uttalelsene, mennesker deler personlige og profesjonelle erfaringer osv. I slike situasjoner vil det altså være så mye informasjon at det kan være vanskelig å fange opp hva som egentlig er essensen. Desto viktigere blir det at ansvarlige aktører er tydelige i sine beskjeder slik at misforståelser og feiltolkninger kan unngås.

Det er flere ting som må balanseres opp mot hverandre i forbindelse med kommunikasjon av terrortrusselen. For det første gjelder det å kommunisere tilstrekkelig informasjon til beslutningstakere, og eventuelt befolkningen, men uten å gi for mye informasjon til eventuelle angripere (Rogers et al., 2007 og Daase og Kessler, 2007). Dette må ses i sammenheng med at trusselaktøren er systematisk og tilpasningsdyktig, og tilgang på informasjon om hvor terrortrusselen vurderes som høy og hvor det er satt inn tiltak, vil trolig gjøre at planene tilpasses dette. Både lokasjon for angrepet og middel for gjennomføring kan endres. Det er åpenbart at dette kan bli en utfordring i forbindelse med balansegangen mellom formidling av risikoinformasjon samtidig som det må sørges for ikke å gi en "oppskrift" på hva som bør ligge til grunn for et vellykket angrep. For det andre gjelder det å vekte informasjonen angående muligheten for at et angrep kan inntreffe og eventuelle konsekvenser det kan få (Simonsen, 2009). Simonsen refererer til at analytikeren, eller den som er ansvarlig for kommunikasjon, er opptatt av å fortelle hvor liten sjanse det er for at et angrep skal inntreffe, mens mottakeren er interessert i å vite mer om konsekvensene. Samtidig forklarer han at mennesker vil vurdere sannsynligheten for at en hendelse skal inntreffe som høyere om konsekvensene er store. Denne balansegangen er vanskelig å opprettholde. Dette framstår som et vanskelig dilemma, og det er vanskelig å si noe om hvordan dette skal hensynstas i kommunikasjonsprosessen. På den ene siden vil det fra kommunikatørens side være riktig å snakke om lav sannsynlighet, om det er dette risikovurderingen viser. På den andre siden må parameterne risikoanalysen er basert på kommuniseres slik at mottakerne med rette også kan gjøre sine egne vurderinger, og hva som ligger til grunn for resultatene. Aven og Renn (2010) understreker at formålet med kommunikasjon av risiko ikke skal være å overbevise tilhørerne om at analytikeren sitter med det eneste riktige svaret, men at det skal bidra til økt forståelse og et bredere beslutningsgrunnlag.

De forskjellige forståelsene og definisjonene av risiko ble redegjort for i kapittel 6.1, og i dette kapitlet ble det tydelig at ulike parametere blir lagt til grunn for risikoanalysen. Dette vil være informasjon som vil være avgjørende å kommunisere slik at mottakerne av informasjonen faktisk vet hva resultatet er basert på. Begrepene usikkerhet og sannsynlighet er heller ikke begreper med én allmenn akseptert tolkning, og bruk av disse begrepene bør forklares for lytteren. I definisjonen av terrorisme mener Hoffman (2006) det er helt nødvendig å forstå at terrorisme er et politisk konsept, og at dette er avgjørende for å skille terrorisme fra andre

voldshandlinger. Dette må også kommuniseres for å tydeliggjøre hvilke handlinger og hendelser det refereres til når det snakkes om terrorisme.

Som vist er for eksempel sannsynlighetsbegrepet omdiskutert både i forbindelse med forståelse og bruk. Ulike forståelser av begrepet gjør at det er helt avgjørende å redegjøre for hva man legger i det når man kommuniserer risiko og usikkerhet med sannsynligheter. I tillegg er det forskjellige måter å bruke sannsynlighet, hvor både verbale og numeriske sannsynligheter gjør seg gjeldende. Uansett om det benyttes tall eller begreper som ”mulig”, ”lav”, ”høy” osv. må det forklares hva de faktisk betyr (Eid og Johnsen, 2005; Aven, Wiencke og Røed, 2007; Fischhoff, 2002 og Hampel;2006). Selv om en risiko vurderes som lav betyr ikke det nødvendigvis at det ikke kan skje, men at det for eksempel er vurdert som mindre sannsynlig enn andre hendelser.

Hvordan mennesker opplever risiko er ikke et enkelt emne, og en del av poenget er at dette vil variere fra person til person og det finnes ingen fasit på hvordan mennesker vil oppfatte risiko (Eid og Johnsen, 2005; Renn, 2008; Aven, 2014; og Fischhoff, 2002). Involvering av interessenter vurderes derfor som en god måte å tilrettelegge for effektiv og forståelig kommunikasjon. Her vil det kunne undersøkes hva for eksempel representanter fra befolkningen, aktuelle virksomheter og andre fagfolk legger i ulike begreper, og hvordan de for eksempel forholder seg til uttalelser angående usikkerhet. Dette vil trolig resultere i at misforståelser og tvetydigheter i meldinger kan oppklares på forhånd, og man kan tilrettelegge for en risikokommunikasjon som i større grad tar høyde for menneskers reaksjoner. I forbindelse med risikoanalyser anses også bruk av ekspertvurderinger og involvering av interessenter som en nyttig metode for å avklare hva som er målet med analysen, hvordan den skal gjennomføres, hva den baserer seg på og, ikke minst, hva de endelige resultatene faktisk betyr.

Den største utfordringen med risikokommunikasjon av terrorisierisikoen, og utgangspunktet for min problemstilling, er usikkerheten. For analytikere vil det kunne oppstå utfordringer i forbindelse frykten for at formidling av usikkerhet skal forveksles med uvitenhet og vaghet (Weiss, 2007 og Bjørnland, 2014b). Det kan også virke som at frykten for at tilhørerne ikke skal forstå usikkerhet er med på å gjøre at formidleren forenkler resultatet fra risikoanalysen, og dermed unngår å snakke om det. Mennesker er vant til å forholde seg til usikkerhet; fra små ting som å gå ut fra hjemmet sitt på morgenen med både solbriller og paraply i veska, til å kjøre bil, reise med fly, hoppe i fallskjerm osv. Aven (2015) argumenterer også for at beslutningstakere i virksomheter er vant til å forholde seg til usikkerhet. Analytikere, eller de som er ansvarlige for kommunikasjon, bør derfor forsøke å formidle usikkerheten på en forståelig måte framfor å tilbakeholde informasjon. Det argumenteres derfor for at å si at man ikke vet er den beste løsningen. Det å tilbakeholde eller uttrykke forenklete resultater kan tilsi at man er mer sikker enn man har grunnlag for, og kan lede til feiltolkninger og mistillit; særlig om det i etterkant kommer fram at analytikeren hadde mer informasjon enn det som ble gitt uttrykk for.

7 Konklusjon

Denne studiens formål var å besvare hvordan man kan kommunisere usikkerheten i risikoanalyser for terrorhendelser. Problemstillingen skulle i så måte gi svar på hvordan man kan kommunisere det man ikke vet. Oppgaven og konklusjonene som trekkes gir ikke alle svarene, men det gis likevel noen gode betraktninger om hva som bør inngå og tas høyde for i kommunikasjon av terrorismerisiko.

Første del av oppgaven omhandlet på hvilken måte ulike risikodefinsjoner og ulike tilnærminger til risiko påvirker hvordan vi forstår og vurderer terrorismerisiko. De ulike definisjonene påvirker hvilke parametere som legges til grunn, og Aven og Renns (2010) definisjon av risiko konkluderes med å være den eneste som eksplisitt tar høyde for usikkerheten som kjennetegner terrorismerisiko. Risikotilnærmingen som kan er forenlig med denne definisjonen er den bayesianske tilnærmingen til risiko. Innenfor denne tilnærmingen anerkjennes både usikkerhet og viktigheten med å formidle bakgrunnskunnskapen for vurderingene. I tillegg åpnes det opp for en kvalitativ tilnærming til risiko, hvor usikkerhetene uttrykkes med subjektive/kunnskapsbaserte sannsynligheter. Det konkluderes også med at sannsynlighetsangivelser er et hensiktsmessig verktøy for å kommunisere resultater fra risikoanalyser, da dette enten eksplisitt eller implisitt, gjennomføres innenfor alle tilnærmingene. Bruk av sannsynligheter, i kombinasjon med forventede konsekvenser, gir også beslutningstakerne mulighet til å prioritere hvilke risikoer som kan aksepteres og hvilke som må håndteres.

I denne oppgaven konkluderes det med at terrorismerisiko er kompleks, usikker og tvetydig, og det anbefales derfor å følge rådene fra Renn (2008) og OECD (2002) angående involvering av interessenter og eksperter. Det konkluderes også med at den bayesianske tilnærmingen til risiko er den eneste som i tilstrekkelig grad tar høyde for opplevd risiko, og i den forbindelse legger til rette for bruk av både ekspertvurderinger og involvering av interessenter. Dette vurderes i denne oppgaven å være en styrke både for en felles risikoforståelse og tilrettelegging for en effektiv og forståelig risikokommunikasjon.

Undersøkelsen av relevante aktørers risikotilnærming har vist at viktige nasjonale aktører innehar forskjellig forståelse av både begreper, framstillingsverktøy og parametere. Det mest hensiktsmessige ville selvsagt vært at en felles språkdrakt hadde vært på plass, men så lenge dette ikke finnes må det legges ekstra vekt på redegjørelse av hva som ligger til grunn for risikovurderingene, uavhengig av hvilken tilnærming som benyttes. Særlig sannsynlighetsbegrepet ser ut til å være befestet med en utdatert forståelse, hvor dette kun oppfattes som en matematisk term som krever kvantitative metoder.

Terrorismerisiko kan gjerne framstilles visuelt, som et supplement til selve risikovurderingen. Dette med forutsetning om at det formidles hva visualiseringen viser og at man tydeliggjør at det kun er en sammenstilling av en langt mer inngående analyse. Trefaktormodellen, eller risikotrekanten, vurderes i denne oppgaven som lite informativ, og det anbefales i denne

oppgaven å benytte bow tie-diagram for hver av risikoene som er vurdert, og til slutt sammenstille disse i en risikomatrise.

Kommunikasjon av terrorismerisikoen og den tilknyttede usikkerheten krever ofte at man må innrømme at man ikke vet. Dette kan være utfordrende for analytikeren både i forbindelse med frykt for tap av stolthet og misoppfatninger hvor dette likestilles med uvitenhet og vaghet. Det konkluderes likevel med at man ikke kan undergrave at det finnes usikkerhet. Videre betyr dette at man i noen tilfeller må si at man ikke vet, og selv om det kan være vanskelig, er dette anbefalingen framfor å tilbakeholde eller forenkle informasjon. Å formidle usikkerheten, og hva denne er knyttet til, konkluderes som å være den beste framgangsmåten både for å ta høyde for tillit hos tilhørerne og å unngå å skape unødig frykt.

Forslag til videre forskning

Temaet for denne oppgaven er beskrevet som et tema det ikke er forsket på så mye fra før av. Dette leder til at det for videre forskning finnes mange aktuelle problemstillinger. Det som kjennetegner den forskningen som eksisterer er at den fokuserer på hva som skiller tilsiktede uønskede handlinger, og terrorhandlinger, fra utilsiktede hendelser. Målet med risikostyring for store og små virksomheter, både i offentlig og privat sektor, er sannsynligvis å kunne ha en helhetlig tilnærming til alle risikoene som kan være aktuelle for dem. Det hadde derfor vært interessant å også rette forskningen mot likhetene mellom de ulike aspektene ved sikkerhet og risiko for å se om man kunne komme nærmere et felles rammeverk. Konklusjonen i denne oppgaven er at den bayesianske tilnærmingen til risiko virker å være mest kompatibel med terrorismerisikoen, og det kunne derfor vært interessant å forsøke å lage et mer konkret rammeverk for risikostyring ut fra denne tilnærmingen.

I diskusjonen ble sikringstiltak mot terrorhendelser nevnt som et potensielt dilemma. Det vil være vanskelig, om ikke umulig, å undersøke effekten av disse da man aldri vet om et terrorangrep hadde skjedd om tiltaket ikke hadde vært implementert. Beslutningsprosessen rundt implementering av tiltak og hva som blir vektlagt i denne prosessen hadde også vært interessant å forske på.

I denne rapporten er det argumentert for at de ulike tilnærmingene kan lede til at risikoanalysen får forskjellige resultater; hvor manglende bruk av sannsynlighet i kombinasjon med konsekvenser for tap av liv kan føre til at risikoen alltid blir høy. På motsatt side leder kun bruk av sannsynlighet og konsekvens, uten hensyn til usikkerhet, til at risikoen kanskje framstilles som feilaktig lav. En interessant studie kunne derfor vært å gjennomføre en komparativ studie hvor man gjennomfører risikoanalyser basert på de ulike tilnærmingene for samme system eller objekt. På denne måten kunne man sammenligne resultater, og sett hvilke parametere som har mest betydning for resultatene.

Referanser

Albrechtsen, E., (2003). *Security vs Safety*. NTNU- Department of Industrial Economics and Technology Management. [pdf] Tilgjengelig på: <http://www.iot.ntnu.no/users/albrecht/rapporter/notat%20safety%20v%20security.pdf> [Sist besøkt 15. mai]

Aven, T. og Krohn, B. S., (2013). A new perspective on how to understand, assess and manage risk and the unforeseen. *Reliability Engineering and system safety*. Vol. 121: 1-10. Universitetet i Stavanger.

Aven, T. og Renn, O., (2010). *Risk Management and Risk Governance. Concepts, Guidelines and Application*. New York: Springer

Aven, T., (2003). *Foundation of Risk Analysis*. New York: Wiley.

Aven, T., (2010). On how to define, understand and describe risk. *Reliability Engineering and System Safety* 95 (2010) s. 632-631.

Aven, T., (2012a). The risk concept – historical and recent development trends. *Reliability Engineering and System Safety* 99 (2012): 33-44.

Aven, T., (2012b). “Risikoteknikken er fullstendig foreldet”, i Aftenposten 20.august 2012. [url] Tilgjengelig på: <http://www.aftenbladet.no/meninger/Risikoteknikken-er-fullstendig-foreldet-3015836.html> [Sist besøkt 25. mai]

Aven, T., (2014). *Risk, surprises and black swans. Fundamental ideas and concepts in risk assessments and risk management*. New York: Routledge.

Aven, T., (2015). *Risikostyring*. Oslo: Universitetsforlaget AS.

Aven, T., Baraldi, P., Flage, R. og Zio, E., (2014). *Uncertainty in Risk Assessment*. West Sussex: John Wiley & Sons Ltd.

Aven, T., Boyesen, M., Njå, O., Olsen, H. O. og Sandve, K., (2004). *Samfunnsikkerhet*. Oslo: Universitetsforlaget AS.

Aven, T., Røed, W. og Wiencke, H. S., (2008). *Risikoanalyse*. Oslo: Universitetsforlaget.

Aven, T., (2016) “Risikomatrix” i Store Norske Leksikon, [url] Tilgjengelig på: <https://snl.no/risikomatrix> [Sist besøkt 25. mai]

Barane, J., (2014). “Et rasjonelt valg – om trefaktortilnærmingen til sikringsrisiko”. [url] Tilgjengelig på: <http://www.proakt.no/#!Et-rasjonelt-valg-%E2%80%93-om-trefaktortilnærmingen-til-sikringsrisiko>

[trefaktortilnC3%A6rmingen-til-sikringsrisiko/sjb0p/56e48feb0cf210a438671766](http://www.pst.no/media/pressemeldinger/trusselen-er-svekket/) [Sist besøkt 25. mai]

Beck, U., (2006). Living in the world risk society. *Economy and Society* Volume 35 Number 3 August 2006: 329-345.

Bjørnland, B., (2014a). “Trusselen er svekket”. [url] Tilgjengelig på: <http://www.pst.no/media/pressemeldinger/trusselen-er-svekket/> [Sist besøkt 02. juni]

Bjørnland, B., (2014b). “PSTs “vage” ordbruk”. [url] Tilgjengelig på: <http://www.pst.no/blogg/psts-vage-ordbruk/> [Sist besøkt 02. juni]

Blaikie, N., (2009). *Designing Social Research*. 2. Utgave. Cambridge: Polity Press

Brun, W. og Teigen, K. H., (1995). Yes, but it is uncertain: Direction and communicative intention of verbal probabilistic terms. *Acta Psychologica* 88 (1995) s. 233-258.

Busmundrud, O., Maal, M., Kiran, J.H og Endregard, M., (2015). Tilnærming til risikovurderinger for tilsiktede uønskede hendelser. FFI-rapport 2015/00923: Kjeller.

Daase, C. og Kessler, O., (2007). Knowns and Unknowns in the “War on Terror”: Uncertainty and the Political Construction of Danger. *SAGE Publications* Vol. 38(4): 411-434.

Danermark et al., (1997). Generalisering, vetenskapeliga slutledningar och modeller för förklarande samhällsvetenskap. Fra Danermark et al. (1997), Att förklare samhället. Lund: Studentlitteratur.

Dreyfus H. L. og Dreyfus S. E., (2005). Expertise in Real World Context. *Organization Studies* 26(5): 779-792.

DSB, (2013) Nasjonalt risikobilde 2013. [pdf] Tilgjengelig på: http://www.dsb.no/Global/Publikasjoner/2013/Tema/NRB_2013.pdf [Sist besøkt 30. november]

DSB, (2014). Nasjonalt risikobilde 2014. [pdf] Tilgjengelig på: http://www.dsb.no/Global/Publikasjoner/2014/Tema/NRB_2014.pdf [Sist besøkt 30. november]

DSB, (2015). Fremgangsmåte for utarbeidelse av Nasjonalt risikobilde (NRB). [pdf] Tilgjengelig på: http://www.dsb.no/Global/Publikasjoner/2015/Tema/Fremgangsmaate_utarbeidelse_nasjonalt_risikobilde.pdf [Sist besøkt 16. desember]

Eid, J. og Johnsen, B. H. ed., (2006). *Operativ psykologi*. Bergen: Fagbokforlaget Vigmostad & Bjørke AS.

Engen, O. A. og Pettersen, K., (2010). *Rethinking risk theory: a critical realist approach to*

aviation security. Universitetet i Stavanger.

Fischhoff, B., (2002): Assessing and Communicating the Risks of Terrorism. [pdf] Tilgjengelig på:
<http://www.orau.gov/cdcynergy/erc/content/activeinformation/resources/FischhoffAAAS.pdf>
[Sist besøkt 03. juni]

Flage, R. og Aven, T., (2009). Expressing and communicating uncertainty in relation to quantitative risk analysis. *R&RATA #2 part 1* (Vol. 2) 2009, June: 9-18.

Flesvik, J. H., (2014a). "Om sannsynlighet for terror" i Dagens Næringsliv 1. desember 2014.
[url] Tilgjengelig på: <http://www.dn.no/meninger/debatt/2014/12/01/2158/Terror/om-sannsynlighet-for-terror> [Sist besøkt 25. mai]

Flesvik, J. H., (2014b). "PST må ut med terrorinfo" i Dagens Næringsliv 17. november 2014.
[url] Tilgjengelig på: <http://www.dn.no/meninger/debatt/2014/11/17/2159/Terror/pst-m-ut-med-terrorinfo> [Sist besøkt 25. mai]

Grønmo, S., (2004). *Samfunnsvitenskapelige metoder*. Bergen: Fagbokforlaget.

Hampel, J., (2006). Different concepts of risk – A challenge for risk communication. *International Journal of Medical Microbiology* 296 (2006) S1, 5-10.

Hoffman, B., (2006). *Inside Terrorism*. Revised and expanded edition. New York: Cloumbia University Press.

Hoffmann, J. F., (2016). Intervju med Jon Fitje Hoffmann, PST. Utført 17. mars 2016.

Hoffmann, J. F., (2016). "Terrortrusselen og nasjonalt nivå". [url] Tilgjengelig på:
<http://www.pst.no/blogg/trusselniva/> [Sist besøkt 02. juni]

Hultgren, G., (2014). "Aldri vært større terror-fare i Norge", i Dagbladet 25. november. [url]
Tilgjengelig på:
http://www.dagbladet.no/2014/11/24/nyheter/terror/pst/terrortrussel/bevepnet_politi/36398929/
[Sist besøkt 25. mai]

Investopedia (a). "Pure Risk". [url] Tilgjengelig på:
<http://www.investopedia.com/terms/p/purerisk.asp> [Sist besøkt 25. mai]

Investopedia (b). "Speculative risk". [url] Tilgjengelig på:
<http://www.investopedia.com/terms/s/speculativerisk.asp> [Sist besøkt 25. mai]

Jacobsen, Dag I., (2005). *Hvordan gjennomføre undersøkelser? Innføring i samfunnsvitenskapelig metode*. 2. utgave Kristiansand: Høyskoleforlaget AS.

JD, (2015a). FoU-strategi for justis- og beredskapssektoren 2015-2019. [pdf] Tilgjengelig på:
http://www.regjeringen.no/contentassets/302c6a76442a46d1b785d9399c399c19/jd_fou-

[strategi_2015-2019.pdf](#) [Sist besøkt 25. mai]

JD, (2015b). FoU-strategi for samfunnssikkerhet 2015-2019. [pdf] Tilgjengelig på: https://www.regjeringen.no/contentassets/f9c80a1b162f4ccca08b7acfa5df9f4a/jd_fou-strategi-for-samfunnssikkerhet_2015-2019.pdf [Sist besøkt 25. mai]

Jenkins, B. M., Willis, H. H og Han, B., (2016). Do Significant Terrorist Attacks Increase the Risk of Further Attacks? [pdf] Tilgjengelig på: [file:///C:/Users/jbr/Downloads/RAND_PE173%20\(1\).pdf](file:///C:/Users/jbr/Downloads/RAND_PE173%20(1).pdf) [Sist besøkt 03. juni]

Jore, S. H. og Njå, O., (2010). Risk of Terrorism: A Scientifically Valid Phenomenon or a Wild Guess? The Impact of Different Approaches to Risk Assessment: Universitetet i Stavanger.

Jore, S. H., (2012). Counterterrorism as Risk Management Strategies. PhD Thesis UIS no. 178 - Faculty of science and technology. Universitetet i Stavanger.

Justis- og politidepartementet (2006) Når sikkerhet er viktigst. –Beskyttelse av landets kritiske infrastrukturer og kritiske samfunnsfunksjoner. Oslo, NOU 6:2006.

Kahneman, D., (2012). *Tenke, fort og langsomt*. Danmark: Pax forlag.

Kaufmann, G. og Kauffmann, A., (2003). *Psykologi i organisasjon og ledelse*. 3. utgave. Bergen: Fagboklaget Vigmostad og Bjørke AS.

Kasperson, R. E., Pidgeon, N. og Slovic, P., (2003). *The Social Amplification of Risk*. Cape Town: Cambridge University Press.

Kessler, O. og Daase, C., (2008). From Insecurity to Uncertainty: Risk and the Paradox of Security Politics. *Alternatives* 33 (2008), s. 211-232.

Lilleåsen, L. R., (2014). “Det kommer ingen ny offentlig trusselvurdering i dag”. [url] Tilgjengelig på: <http://www.pst.no/blogg/psts-vage-ordbruk/> [Sist besøkt 02. juni]

Liu, B. F. et al., (2016). Communicating crises uncertainty: A review of the knowledge gaps. *Public Relations Review*. 2016: 1-9. [pdf] Tilgjengelig på: http://ac.els-cdn.com/S0363811116300327/1-s2.0-S0363811116300327-main.pdf?_tid=39a3785c-297e-11e6-85c0-00000aab0f02&acdnat=1464953459_929f546f115905f2833e69044b0dddc5 [Sist besøkt 03. juni]

Midtgård, A. K., (2016). Intervju med Ann Karin Midtgård, DSB. Utført: 23. februar 2016.

Mærli, M. B., (2014). “Usannsynlig sannsynlig” i Dagens Næringsliv 23.november 2014. [url] Tilgjengelig på: <http://www.dn.no/meninger/debatt/2014/11/23/2058/Terror/usannsynlig-sannsynlig> [Sist besøkt 25. mai]

Norsk senter for prosjektledelse. “Usikkerhet, risiko og muligheter”. [url] Tilgjengelig på: <http://www.nsp.ntnu.no/index.php?pageId=430> [Sist besøkt 25. mai]

NOU (2012). Rapport fra 22.juli kommisjonen. Oslo, NOU 2012:14.

NS 5814, (2008). Krav til risikovurderinger. Norsk standard NS 5814:2008.

NS 5830, (2012): Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Terminologi. Norsk Standard NS 5830:2012.

NS 5832, (2014). Samfunnssikkerhet – Beskyttelse mot tilsiktede uønskede handlinger – Krav til sikringsrisikoanalyse. Norsk standard NS 5832:2014

NS-ISO 31000, (2009). Risikostyring. Metoder for risikovurderinger. Norsk Standard NS-ISO/IEC31010:2009.

NSM (2014) Sikkerhetstilstanden 2014. [pdf] Tilgjengelig på: https://nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/rst_2014.pdf [Sist besøkt 20. november]

NSM, (2016a). Håndbok for risikovurdering for sikring. Nasjonal sikkerhetsmyndighet, mars 2016.

NSM, (2016b). Kan risiko styres? [pdf] Tilgjengelig på: https://www.nsm.stat.no/globalassets/rapporter/rapport-om-sikkerhetstilstanden/nsm_risiko_2016.pdf [Sist besøkt 02. juni]

NSM, POD og PST, (2015): En veileder i sikrings- og beredskapstiltak mot tilsiktede uønskede handlinger. Oslo.

OECD, (2002). OECD Guidance document on risk communication for chemical risk management. [pdf] Tilgjengelig på: [http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=env/jm/mono\(2002\)18](http://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?doclanguage=en&cote=env/jm/mono(2002)18) [Sist besøkt 02. juni]

Olsen, B., (2012). “Risiko – en innføring”. [url] Tilgjengelig på: <http://www.pst.no/blogg/risiko-en-innforing/> [Sist besøkt 02. juni]

Pettersen, K. og Engen, O. A., (2010). Rethinking risk theory: a critical realist approach to aviation security. Universitetet i Stavanger.

PST, (2016). Åpen trusselvurdering 2016. [pdf] Tilgjengelig på: http://www.pst.no/media/81096/PST_Brosjyre_Trussel_NORSK.pdf [Sist besøkt 08. juni]

Pst.no. “Trusselvurderinger”. [url] Tilgjengelig på:

http://www.pst.no/media/74351/PSTs_tv2015-2.pdf [Sist besøkt 6. juni]

Rapp, C., (2014) "Terror vanskelig å forutse" i Dagens Næringsliv 24.november 2014. [url] Tilgjengelig på: <http://www.dn.no/meninger/debatt/2014/11/24/2159/Terror/terror-vanskelig--forutse> [Sist besøkt 25. mai]

Raussand, M. og Utne, B. I., (2009). *Risikoanalyse –teori og metoder*. Bergen: Fagboklaget.

Renn, O., (2004). Perception of risks. *Toxicology Letters* 149 (2004): 405-413.

Renn, O., (2008). *Risk Governance. Coping with Uncertainty in a Complex World*. Earthscan: London.

Rogers, M. B. et al., (2007). Mediating the social and psychological impacts of terrorist attacks: The role of risk perception and risk communication. *International Review of Psychiatry*, June 2007; 19(3): 279-288.

Simonsen, A., (2009). "Risikokommunikasjon". [url] Tilgjengelig på: <http://www.kommunikasjon.no/fagstoff/krisekommunikasjon/risiko-og-krisekommunikasjon> [Sist besøkt 03. juni]

Slovic, P. og Weber, E. U., (2002). Perception of Risk Posed by Extreme Events. [pdf] Tilgjengelig på: <http://www.rff.org/files/sharepoint/Documents/Events/Workshops%20and%20Conferences/Cli%20mate%20Change%20and%20Extreme%20Events/slovic%20extreme%20events%20final%20ge%20neva.pdf> [Sist besøkt 02. juni]

Statoil, (2013): The In Amenas Attack. Report of the investigation into the terrorist attack on In Amenas. Prepared for Statoil ASA's board of directors. [pdf] Tilgjengelig på: <http://www.statoil.com/en/NewsAndMedia/News/2013/Downloads/In%20Amenas%20report.pdf> [Sist besøkt 25. mai]

Thagaard, T., (2009). *Systematikk og innlevelse en innføring i kvalitativ metode*. 3. utgave. Bergen: Bokforlaget.

Vastveit, K., Njå, O., Braut, G. S. og Holte, M. R., (2012). A discussion on expert judgements in national risk analyses. *Advances in Safety, Reliability and Risk Management* 2012:1407-1415.

Weiss, C., (2007) Communicating Uncertainty in Intelligence and Other Professions. *International Journal of Intelligence and CounterIntelligence*, 21: 57-85, 2008.

Yin, R. K. (2014). *Case Study Research. Design and Methods*. 5. utgave. London: Sage Publications.

About FFI

The Norwegian Defence Research Establishment (FFI) was founded 11th of April 1946. It is organised as an administrative agency subordinate to the Ministry of Defence.

FFI's MISSION

FFI is the prime institution responsible for defence related research in Norway. Its principal mission is to carry out research and development to meet the requirements of the Armed Forces. FFI has the role of chief adviser to the political and military leadership. In particular, the institute shall focus on aspects of the development in science and technology that can influence our security policy or defence planning.

FFI's VISION

FFI turns knowledge and ideas into an efficient defence.

FFI's CHARACTERISTICS

Creative, daring, broad-minded and responsible.

Om FFI

Forsvarets forskningsinstitutt ble etablert 11. april 1946. Instituttet er organisert som et forvaltningsorgan med særskilte fullmakter underlagt Forsvarsdepartementet.

FFIs FORMÅL

Forsvarets forskningsinstitutt er Forsvarets sentrale forskningsinstitusjon og har som formål å drive forskning og utvikling for Forsvarets behov. Videre er FFI rådgiver overfor Forsvarets strategiske ledelse. Spesielt skal instituttet følge opp trekk ved vitenskapelig og militærteknisk utvikling som kan påvirke forutsetningene for sikkerhetspolitikken eller forsvarsplanleggingen.

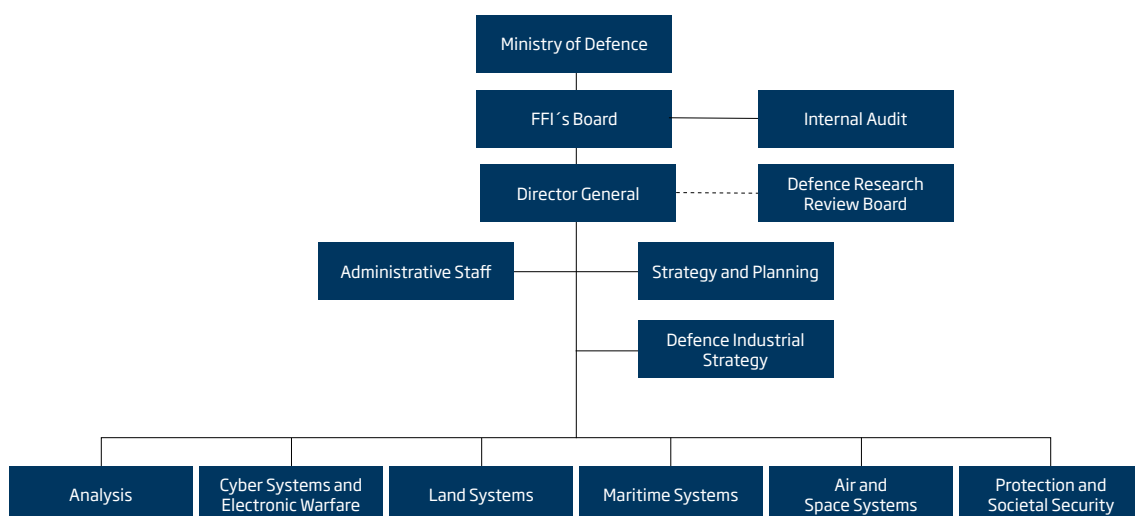
FFIs VISJON

FFI gjør kunnskap og ideer til et effektivt forsvar.

FFIs VERDIER

Skapende, drivende, vidsynt og ansvarlig.

FFI's organisation



Forsvarets forskningsinstitutt
Postboks 25
2027 Kjeller

Besøksadresse:
Instituttveien 20
2007 Kjeller

Telefon: 63 80 70 00
Telefaks: 63 80 71 15
Epost: ffi@ffi.no

Norwegian Defence Research Establishment (FFI)
P.O. Box 25
NO-2027 Kjeller

Office address:
Instituttveien 20
N-2007 Kjeller

Telephone: +47 63 80 70 00
Telefax: +47 63 80 71 15
Email: ffi@ffi.no